SOPHOS

simple + secure

Sophos UTM

管理ガイド

製品バージョン:9.100

ドキュメント作成日:2013年10月7日

当文書に記載されている仕様と情報は、予告なく変更される場合があります。例で使用されている会社、名前、データは、明記されている場合を除き架空のものです。Astaro GmbH & Co. KG の書面による明示的な許可なく、当文書の一部または全体を手段を問わず複製または配布することは、いかなる理由においても許可されません。本マニュアル原文の翻訳には、「マニュアル原文の翻訳(Translation of the original manual) 」と記載しなければなりません。

© 2000–2013 Astaro GmbH & Co. KG.
All rights reserved.
Amalienbadstraße 41/Bau 52,
76227 Karlsruhe,
Germany
http://www.sophos.co.jp

Sophos UTM、Sophos UTM Manager、Astaro Security Gateway、Astaro Command Center、Astaro Gateway Manager、および WebAdmin は、Astaro GmbH & Co. KG の登録商標です。Cisco は、Cisco Systems Inc. の登録商標です。iOS は、Apple Inc. の登録商標です。Linux は、Linus Torvalds の登録商標です。他のすべての商標は、該当する所有者の財産です。

限定保証

当文書に記載されている情報の正確性は保証されません。コメントや修正については、nsg-docu@sophos.comまでご連絡ください。

目次

1 インストール **15**

1.1 参考資料 15
1.2 システム要件 15
1.2.1 UPS デバイスのサポート 16
1.2.2 RAID サポート 17
1.3 インストール手順 17
1.3.1 インストール中の主な機能 17
1.3.2 インストール中の特別なオプション 18
1.3.3 インストール Sophos UTM 18
1.4 基本設定 21
1.5 バックアップリストア 26

2 WebAdmin **29**

2.1 WebAdmin メニュー 30
2.2 ボタンバー 31
2.3 リスト 32
2.4 リストの検索 33
2.5 ダイアログボックス 34
2.6 ボタンとアイコン 35
2.7 オブジェクトリスト 37

3 ダッシュボード **39**

3.1 ダッシュボード設定 41
3.2 フローモニタ 42

4 マネジメント **47**

4.1 システム設定 47
4.1.1 組織 48
4.1.2 ホスト名 48
4.1.3 日付と時刻 48
4.1.4 シェルアクセス 51
4.1.5 スキャン設定 52
4.1.6 設定またはパスワードのリセット 52
4.2 WebAdmin 設定 53
4.2.1 一般 53
4.2.2 アクセス制御 54
4.2.3 HTTPS 証明書 55
4.2.4 ユーザ設定 56
4.2.5 詳細 57

4.3 ライセンス ... 59
4.3.1 ライセンスの取得方法 ... 59
4.3.2 ライセンスモデル ... 61
4.3.3 概要 ... 64
4.3.4 インストール ... 65
4.3.5 アクティブな IP アドレス ... 66
4.4 Up2Date ... 66
4.4.1 概要 ... 66
4.4.2 設定 ... 68
4.4.3 詳細 ... 69
4.5 バックアップ/リストア ... 70
4.5.1 バックアップ/リストア ... 70
4.5.2 自動バックアップ ... 73
4.6 ユーザポータル ... 74
4.6.1 グローバル ... 77
4.6.2 詳細 ... 77
4.7 通知 ... 78
4.7.1 グローバル ... 79
4.7.2 通知 ... 79
4.7.3 詳細 ... 79
4.8 カスタマイズ ... 80
4.8.1 グローバル ... 80
4.8.2 Web メッセージ ... 82
4.8.2.1 Web メッセージの修正 ... 84
4.8.2.2 ダウンロードマネージャ ... 84
4.8.3 Web テンプレート ... 85
4.8.3.1 Web テンプレートのカスタマイズ ... 85
4.8.3.2 カスタム Web テンプレートと画像のアップロード ... 86
4.8.4 メールメッセージ ... 86
4.9 SNMP ... 87
4.9.1 クエリ ... 88
4.9.2 トラップ ... 89
4.10 集中管理(HA) ... 90
4.10.1 Sophos UTM Manager ... 90
4.11 冗長化(HA) ... 93
4.11.1 ハードウェアとソフトウェアの要件 ... 94
4.11.2 ステータス ... 95
4.11.3 システムステータス ... 96
4.11.4 設定 ... 96
4.12 シャットダウンとリスタート ... 100

5 定義とユーザ **101**

5.1 ネットワーク定義 101
5.1.1 ネットワーク定義 101
5.1.2 MAC アドレス定義 106
5.2 サービス定義 107
5.3 時間帯定義 109
5.4 ユーザとグループ 110
5.4.1 ユーザ 110
5.4.2 グループ 113
5.5 クライアント認証 115
5.6 認証サーバ 117
5.6.1 グローバル設定 117
5.6.2 サーバ 118
5.6.2.1 eDirectory 119
5.6.2.2 Active Directory 120
5.6.2.3 LDAP 123
5.6.2.4 RADIUS 124
5.6.2.5 TACACS+ 126
5.6.3 シングルサインオン 127
5.6.4 詳細 129

6 インタフェースとルーティング **131**

6.1 インタフェース 131
6.1.1 インタフェース 132
6.1.1.1 自動インタフェースネットワーク定義 133
6.1.1.2 インタフェースタイプ 133
6.1.1.3 グループ 135
6.1.1.4 3G/UMTS 136
6.1.1.5 イーサネットスタティック 138
6.1.1.6 イーサネット VLAN 140
6.1.1.7 イーサネット DHCP 142
6.1.1.8 DSL (PPPoE) 143
6.1.1.9 DSL (PPPoA/PPTP) 146
6.1.1.10 モデム (PPP) 148
6.1.2 追加アドレス 150
6.1.3 リンクアグリゲーション 151
6.1.4 アップリンクバランシング 152
6.1.5 マルチパスルール 156
6.1.6 ハードウェア 158
6.2 ブリッジ 160
6.2.1 ステータス 160
6.2.2 詳細 161

6.3 QoS 162
6.3.1 ステータス 162
6.3.2 トラフィックセレクタ 164
6.3.3 帯域幅プール 168
6.3.4 ダウンロード帯域幅調整 169
6.3.5 詳細 170
6.4 アップリンクモニタリング 171
6.4.1 グローバル 171
6.4.2 アクション 172
6.4.3 詳細 173
6.5 IPv6 175
6.5.1 グローバル 176
6.5.2 プレフィックス広告 176
6.5.3 再割り当て 177
6.5.4 6to4 178
6.5.5 トンネルブローカー 179
6.6 スタティックルーティング 180
6.6.1 標準スタティックルート 180
6.6.2 ポリシールート 181
6.7 OSPF 183
6.7.1 グローバル 183
6.7.2 エリア 184
6.7.3 インタフェース 186
6.7.4 メッセージダイジェスト 187
6.7.5 デバッグ 188
6.7.6 詳細 188
6.8 BGP 189
6.8.1 グローバル 190
6.8.2 システム 190
6.8.3 ネイバー 191
6.8.4 ルートマップ 193
6.8.5 フィルタリスト 194
6.8.6 詳細 195
6.9 マルチキャストルーティング (PIM-SM) 196
6.9.1 グローバル 197
6.9.2 インタフェース 198
6.9.3 RPルータ 199
6.9.4 ルート 199
6.9.5 詳細 200

7 ネットワークサービス **203**

7.1 DNS 203
7.1.1 グローバル 203
7.1.2 フォワーダ 204
7.1.3 リクエストルーティング 205
7.1.4 スタティックエントリ 205
7.1.5 DynDNS 205
7.2 DHCP 208
7.2.1 サーバ 208
7.2.2 リレー 211
7.2.3 スタティックマッピング 212
7.2.4 IPv4 リーステーブル 212
7.2.5 IPv6 リーステーブル 213
7.2.6 オプション 215
7.3 NTP 217

8 ネットワークプロテクション 219

8.1 ファイアウォール 219
8.1.1 ルール 219
8.1.2 送受信国別ブロック 223
8.1.3 送受信国除外 224
8.1.4 ICMP 225
8.1.5 詳細 226
8.2 NAT 229
8.2.1 マスカレード 229
8.2.2 NAT 230
8.3 侵入防御(IPS) 233
8.3.1 グローバル 234
8.3.2 攻撃パターン 235
8.3.3 DoS/フラッド防御 236
8.3.4 ポートスキャン防御 238
8.3.5 除外 239
8.3.6 詳細 241
8.4 サーバロードバランシング 242
8.4.1 分散ルール 242
8.5 VoIP 245
8.5.1 SIP 245
8.5.2 H.323 246
8.6 詳細 247
8.6.1 ジェネリックプロキシ 247
8.6.2 SOCKS プロキシ 248
8.6.3 IDENTリバースプロキシ 249

9 Web プロテクション **251**

9.1 Web フィルタリング 252
9.1.1 グローバル 252
9.1.2 ウイルス/マルウェア対策 256
9.1.3 URL フィルタリング 257
9.1.4 URL フィルタリングカテゴリ 261
9.1.5 除外 262
9.1.6 詳細 264
9.1.7 HTTPS CA 270
9.2 Web フィルタリングプロファイル 273
9.2.1 概要 274
9.2.2 プロキシプロファイル 275
9.2.3 フィルタ割当て 280
9.2.4 フィルタアクション 281
9.2.5 親プロキシ 285
9.3 アプリケーションコントロール 286
9.3.1 ネットワーク可視化 286
9.3.2 アプリケーションコントロールルール 287
9.3.3 詳細 289
9.4 FTP 290
9.4.1 グローバル 290
9.4.2 ウイルス対策 291
9.4.3 除外 292
9.4.4 詳細 293

10 Eメールプロテクション **295**

10.1 SMTP 295
10.1.1 グローバル 295
10.1.2 ルーティング 296
10.1.3 ウイルス対策 298
10.1.4 スパム対策 301
10.1.5 除外 306
10.1.6 リレー 307
10.1.7 詳細 309
10.2 SMTP プロファイル 312
10.3 POP3 316
10.3.1 グローバル 316
10.3.2 ウイルス対策 317
10.3.3 スパム対策 318
10.3.4 除外 319
10.3.5 詳細 320

10.4 暗号化 325
10.4.1 グローバル 327
10.4.2 オプション 328
10.4.3 内部ユーザ 329
10.4.4 S/MIME 認証局 331
10.4.5 S/MIME 証明書 332
10.4.6 OpenPGP 公開鍵 333
10.5 隔離レポート 334
10.5.1 グローバル 335
10.5.2 除外 336
10.5.3 詳細 337
10.6 メールマネージャ 338
10.6.1 メールマネージャウィンドウ 339
10.6.1.1 SMTP/POP3 隔離 339
10.6.1.2 SMTP Spool 341
10.6.1.3 SMTP ログ 342
10.6.2 グローバル 343
10.6.3 設定 344

11 エンドポイントプロテクション 347

11.1 コンピュータ管理 349
11.1.1 グローバル 349
11.1.2 エージェントの導入 350
11.1.3 コンピュータの管理 351
11.1.4 グループ管理 352
11.1.5 詳細 354
11.2 ウイルス対策 354
11.2.1 ポリシー 354
11.2.2 除外 356
11.3 デバイスコントロール 358
11.3.1 ポリシー 358
11.3.2 除外 359
11.4 Webコントロール 361
11.4.1 グローバル 362
11.4.2 詳細 362
11.4.3 対応していない機能 362

12 ワイヤレスプロテクション 365

12.1 グローバル設定 366
12.1.1 グローバル設定 366
12.1.2 詳細 367
12.2 ワイヤレスネットワーク 367

12.3 アクセスポイント 371
12.3.1 概要 372
12.3.2 グループ化 376
12.4 メッシュネットワーク 377
12.5 ワイヤレスクライアント 380
12.6 ホットスポット 381
12.6.1 グローバル 382
12.6.2 ホットスポット 383
12.6.3 バウチャー定義 385
12.6.4 詳細 386

13 Web サーバプロテクション 387

13.1 WAF 387
13.1.1 グローバル 387
13.1.2 仮想 Web サーバ 388
13.1.3 バックエンドWebサーバ 390
13.1.4 ファイアウォールプロファイル 391
13.1.5 除外 395
13.1.6 サイトパスルーティング 396
13.1.7 詳細 398
13.2 証明書管理 398
13.2.1 証明書 398
13.2.2 認証局 (CA) 398
13.2.3 証明書失効リスト(CRL) 399
13.2.4 詳細 399

14 RED マネジメント 401

14.1 概要 402
14.2 グローバル設定 402
14.3 [サーバ] クライアントマネジメント 403
14.4 [サーバ] 導入ヘルパ 410
14.5 [クライアント] トンネルマネジメント 413

15 サイト間 VPN 415

15.1 Amazon VPC 416
15.1.1 ステータス 416
15.1.2 セットアップ 417
15.2 IPsec 418
15.2.1 コネクション 421
15.2.2 リモートゲートウェイ 422
15.2.3 ポリシー 425
15.2.4 ローカル RSA 鍵 428

15.2.5 詳細 429
15.2.6 デバッグ 431
15.3 SSL 432
15.3.1 コネクション 432
15.3.2 設定 434
15.3.3 詳細 435
15.4 証明書管理 436
15.4.1 証明書 437
15.4.2 認証局 439
15.4.3 証明書失効リスト(CRL) 440
15.4.4 詳細 440

16 リモートアクセス 443

16.1 SSL 444
16.1.1 プロファイル 444
16.1.2 設定 445
16.1.3 詳細 446
16.2 PPTP 448
16.2.1 グローバル 448
16.2.2 iOS デバイス 450
16.2.3 詳細 450
16.3 L2TP over IPsec 451
16.3.1 グローバル 451
16.3.2 iOS デバイス 454
16.3.3 デバッグ 454
16.4 IPsec 455
16.4.1 コネクション 458
16.4.2 ポリシー 459
16.4.3 詳細 463
16.4.4 デバッグ 465
16.5 HTML5 VPN ポータル 465
16.5.1 グローバル 466
16.6 Cisco VPN クライアント 469
16.6.1 グローバル 469
16.6.2 iOS デバイス 470
16.6.3 デバッグ 471
16.7 詳細 472
16.8 証明書管理 472
16.8.1 証明書 473
16.8.2 認証局 (CA) 473
16.8.3 証明書失効リスト(CRL) 473

16.8.4 詳細 473

17 ログとレポート **475**

17.1 ログファイルの閲覧 477
17.1.1 今日のログファイル 477
17.1.2 アーカイブログファイル 477
17.1.3 ログファイルの検索 478
17.2 ハードウェア 478
17.2.1 デイリー 478
17.2.2 ウィークリー 479
17.2.3 マンスリー 479
17.2.4 年次 479
17.3 ネットワーク使用状況 479
17.3.1 デイリー 480
17.3.2 ウィークリー 480
17.3.3 マンスリー 480
17.3.4 年次 480
17.3.5 帯域使用状況 480
17.4 ネットワークプロテクション 482
17.4.1 デイリー 482
17.4.2 ウィークリー 482
17.4.3 マンスリー 482
17.4.4 年次 482
17.4.5 ファイアウォール 483
17.4.6 IPS 483
17.5 Webプロテクション 484
17.5.1 Web 使用状況レポート 484
17.5.2 検索エンジンレポート 487
17.5.3 部門 490
17.5.4 スケジュールレポート 491
17.5.5 アプリケーションコントロール 491
17.5.6 非匿名化 492
17.6 Eメールプロテクション 493
17.6.1 使用状況グラフ 493
17.6.2 メール使用状況 493
17.6.3 ブロックメール 494
17.6.4 非匿名化 494
17.7 ワイヤレスプロテクション 495
17.7.1 デイリー 495
17.7.2 ウィークリー 495
17.7.3 マンスリー 495

17.7.4 年次 496
17.8 リモートアクセス 496
17.8.1 アクティビティ 496
17.8.2 セッション 496
17.9 Web サーバプロテクション 497
17.9.1 使用状況グラフ 497
17.9.2 詳細 497
17.10 エグゼクティブレポート 498
17.10.1 レポートを見る 498
17.10.2 アーカイブエグゼクティブレポート 498
17.10.3 設定 498
17.11 ログ設定 499
17.11.1 ローカルログ 499
17.11.2 Syslog送信ログ選択 500
17.11.3 リモートログファイルアーカイブ 501
17.12 レポート設定 503
17.12.1 設定 503
17.12.2 除外 506
17.12.3 匿名化 507

18 サポート **509**

18.1 ドキュメント 509
18.2 印刷可能形式設定情報 510
18.3 サポート窓口 510
18.4 ツール 511
18.4.1 Ping チェック 511
18.4.2 Traceroute 512
18.4.3 DNS ルックアップ 512
18.5 詳細 513
18.5.1 プロセスリスト 513
18.5.2 LAN コネクション 513
18.5.3 ルーティングテーブル 513
18.5.4 インタフェーステーブル 513
18.5.5 コンフィグダンプ 514
18.5.6 REF_をリゾルブ 514

19 ログオフ **515**

20 ユーザポータル **517**

20.1 ユーザポータル:隔離メール 517
20.2 ユーザポータル:メールログ 519
20.3 ユーザポータル:POP3 アカウント 520

20.4 ユーザポータル:送信者ホワイトリスト 520
20.5 ユーザポータル:送信者ブラックリスト 521
20.6 ユーザポータル:ホットスポット 521
20.7 ユーザポータル:クライアント認証 524
20.8 ユーザポータル:リモートアクセス 524
20.9 ユーザポータル:HTML5 VPNポータル 524
20.10 ユーザポータル:パスワードの変更 526
20.11 ユーザポータル:HTTPSプロキシ 526

1 インストール

このセクションは、ネットワークへのSophos UTMのインストールとセットアップについての情報を提供します。Sophos UTMのインストールは、2つのステップで行います。まずソフトウェアをインストールし、次に基本システム設定を行います。ソフトウェアのインストールに必要な初期セットアップは、コンソールベースのインストールメニューで行います。内部設定は、管理ワークステーションで、Sophos UTMの Web ベースの管理用インタフェースである WebAdmin を使用して実行できます。インストールを開始する前に、ハードウェアがシステムの最低要件を満たしていることを確認してください。

注 –Sophos UTMハードウェアアプライアンスを使用する場合、次のセクションをスキップして、*基本設定*のセクションに直接進むことができます。この理由は、すべてのSophos UTMハードウェアアプライアンスはUTMソフトウェアがプレインストールされた状態で出荷されるためです。

この章では、次のトピックについて説明します。

- 参考資料
- システム要件
- インストール手順
- 基本設定
- バックアップリストア

1.1 参考資料

インストールを始める前に、Sophos UTM製品の設定の一助となる以下のマニュアルを読むことをお勧めします。いずれのマニュアルも、Sophos UTMハードウェアアプライアンス装置に同梱されています。また、Sophos UTM リソースセンターでもご利用いただけます。

- クイックスタートガイドハードウェア
- 取扱説明書(Operating Instructions)

1.2 システム要件

UTMのインストールおよび使用のための最低限のハードウェア要件は以下のとおりです。

- **プロセッサ:**Pentium 4 (1.5GHz) (あるいは互換のもの)
- **メモリ:**1GB RAM
- **HDD:**20 GB IDE または SCSI ハードディスクドライブ
- **CD-ROM ドライブ:**ブート可能な IDE または SCSI CD-ROMドライブ
- **NIC:**2枚以上の PCI イーサネットネットワークインタフェースカード
- **NIC** (オプション):1枚のハートビート対応 PCI イーサネットネットワークインタフェースカード。冗長化システムでは、プライマリシステムとセカンダリシステムが、いわゆるハートビート要求を介して互いに通信します。冗長化システムをセットアップする場合は、両方のユニットにハートビート対応のネットワークインタフェースカードを装備する必要があります。
- **USB** (オプション):UPS デバイスの通信用に 1つの USB ポート
- **スイッチ** (オプション):ネットワークセグメントの接続 (およびその間の選択) を行うネットワークデバイス。このスイッチはジャンボフレームをサポートすることが必要です。

Sophos では、UTMソフトウェアと互換性を持つハードウェアデバイスのリストを用意しています。*ハードウェア互換性リスト* (HCL) はSophos サポートデータベースからご利用いただけます。UTMソフトウェアのインストールと使用でエラーの発生を防止するために、HCL にリストされたハードウェアのみを使用してください。WebAdmin へのアクセスに使用されるクライアント PC に必要なハードウェアおよびソフトウェアの条件を以下に示します。

- **プロセッサ:**クロック周波数: 1GHz 以上
- **ブラウザ:**最新バージョンの Firefox (推奨)、最新バージョンの Chrome、最新バージョンの Safari、または Microsoft Internet Explorer 8 以降。JavaScript を有効にする必要があります。さらに、UTMの内部ネットワークカードの IP アドレス (eth0) にプロキシを使用しないようにブラウザを設定する必要があります。

1.2.1 UPS デバイスのサポート

無停電電源装置 (UPS) デバイスは、公共の電力が利用できない場合に、別個の電源から接続した機器に電力を供給して給電を維持します。Sophos UTMSophos UTM は、MGE UPS Systems および APC の UPS デバイスをサポートしています。UPS デバイスとSophos UTMの通信は USB インタフェースを介して行われます。

UPS デバイスがバッテリオペレーションを始動すると、管理者に通知が送信されます。停電が長期間続いて UPS デバイスの電圧が限界値に近づいた場合は、管理者に別のメッセージが送信されます。そして、Sophos UTMは自動的にシャットダウンします。

注 – Sophos UTMにUPS デバイスを接続するときは、UPS デバイスの使用説明書をお読みください。UTMのUSB インタフェースを介してブート(起動)すると、UTM は UPS デバイスを認識します。USB インタフェースを相互に接続してからSophos UTMをブートしてください。

1.2.2 RAID サポート

RAID (*Redundant Array of Independent Disks*)とは、複数のハードドライブを使用してドライブ間でデータを共有あるいは複製するデータストレージ技術です。RAID システムが検出されてダッシュボードに正しく表示されるようにするには、Sophos UTMでサポートされる RAID コントローラを使用することが必要です。サポートされている RAID コントローラを確認するには、HCL をチェックしてください。HCL はSophos サポートデータベースで提供されています。「HCL」を検索用語として使用して、該当するページを探してください。

1.3 インストール手順

次に、Sophos UTMソフトウェアのインストールプロセスを順を追って説明します。

インストールを始める前に、次のアイテムがお手元にあることを確認してください。

- Sophos UTM CD-ROM
- Sophos UTMライセンスキー

セットアッププログラムがシステムのハードウェアをチェックしてから、PC にソフトウェアをインストールします。

1.3.1 インストール中の主な機能

メニューのナビゲーションには、次のキーを使用します(画面の下部にも追加のキー機能がリストされています)。

- F1:コンテキストに応じたヘルプ画面が表示されます。
- カーソルキー:これらのキーを使用して、テキストボックス間をナビゲーションします(たとえば、ライセンス条件や、キーボードレイアウトの選択時)。
- Tab キー:テキストボックス、リスト、ボタンを前後に移動します。
- Enter キー:入力した情報が確定され、インストールが次のステップに進みます。
- Space キー:アスタリスク(*)の付いたオプションを選択または選択解除します。

- Alt-F2:インストールコンソールに切り替えます。
- Alt-F4:ログに切り替えます。
- Alt-F1:インタラクティブバッシュシェルに切り替えます。
- Alt-F1:メインのインストール画面に戻ります。

1.3.2 インストール中の特別なオプション

一部の画面には追加のオプションがあります。

ログの閲覧:インストールログを開きます。

サポート:サポートダイアログ画面を開きます。

USB スティックへ:インストールログを zip ファイルとして USB スティックへ書き込みます。このオプションを確定する前に、必ず USB スティックを差し込んでください。この zip ファイルは、インストールでの問題をSophos UTMサポートチームなどが解決する際に使用されます。

戻る:前の画面に戻ります。

キャンセル:インストールの中止を確認するダイアログウィンドウが開きます。

ヘルプ:コンテキストに応じたヘルプ画面が表示されます。

1.3.3 インストール Sophos UTM

1. **CD-ROMドライブから PC をブートします。**
   インストール開始画面が表示されます。

   > **注** – いつでも F1 を押してヘルプメニューを利用することができます。開始画面で F3 を押すと、トラブルシューティングの画面が開きます。

2. **Enter を押します。**
   「*開始*」画面が表示されます。
3. **「*インストール開始*」を選択します。**
   「*ハードウェア検出*」画面が表示されます。

   ソフトウェアが次のハードウェアコンポーネントをチェックします。

   - CPU
   - ハードディスクドライブのサイズとタイプ

- CD-ROMドライブ
- ネットワークインタフェースカード
- IDE または SCSI コントローラ

システムが最低要件を満たしていない場合、エラーが報告され、インストールは中止されます。

ハードウェア検出が完了すると、「*検出されたハードウェア*」画面が参考として表示されます。

4. **Enterを押します。**
「*キーボード選択*」画面が表示されます。

5. **キーボードのレイアウトを選択します。**
カーソルキーを使用してキーボードレイアウト（例: *English (UK)*）を選択し、Enter を押して続行します。

「*タイムゾーン選択*」画面が表示されます。

6. **エリアを選択します。**
カーソルキーを使用してエリア（例: *Europe*）を選択し、Enter を押して続行します。

7. **タイムゾーンを選択します。**
カーソルキーを使用してタイムゾーン（例: *London*）を選択し、Enter を押して続行します。

「*日付と時刻*」画面が表示されます。

8. **日付と時刻を設定します。**
日付と時刻が正しくない場合、ここで変更できます。Tab キーとカーソルキーを使用して、テキストボックス間を切り替えます。「*ホストクロックは UTC*」オプションの選択を解除するには、Space キーを押します。無効なエントリは却下されます。設定を Enter キーで確認します。

「*管理インタフェース選択*」画面が表示されます。

9. **内部ネットワークカードを選択します。**
WebAdmin ツールを使用してSophos UTMの残りの設定を行う場合、内部ネットワークカード（eth0）とするネットワークインタフェースカードを選択します。リストから使用可能なネットワークカードを1つ選択し、Enter キーで選択を確認します。

注 – アクティブな接続があるインタフェースは、*[link]* と表示されます。

「*ネットワーク設定*」画面が表示されます。

10. **管理ネットワークインタフェースを設定します。**
管理ネットワークインタフェースとする内部インタフェースの IP アドレス、ネットワークマスク、ゲートウェイを定義します。デフォルト値は以下のとおりです。

アドレス:192.168.2.100

ネットマスク:255.255.255.0

ゲートウェイ:なし

ネットマスクで定義されたサブネット外にあるワークステーションから WebAdmin インタフェースを使用したい場合のみ、ゲートウェイ値を変更する必要があります。ゲートウェイ自体がサブネット内にある必要があります。[1]

設定を Enter キーで確認します。

CPU が 64 ビットをサポートしている場合、「*64ビットカーネルのサポート*」画面が表示されます。サポートしていない場合、続いて「*Enterprise Toolkit*」画面が表示されます。

11. **64ビットカーネルをインストールします。**
「*はい*」を選択すると64ビットカーネルが、「*いいえ*」をインストールすると32ビットカーネルがインストールされます。

「*Enterprise Toolkit*」画面が表示されます。

12. **Enterprise Toolkit のインストールに同意します。**
Enterprise Toolkit はSophos UTMソフトウェアから構成されています。Open Source ソフトウェアのインストールのみを決定できます。ただし、Sophos UTMの全機能を使用するためには、Enterprise Toolkit もインストールすることをお勧めします。

Enter を押して両方のソフトウェアパッケージをインストールするか、「*いいえ*」を選択して Open Source ソフトウェアのみをインストールします。

インストール:「*パーティショニング*」画面が表示されます。

[1]たとえば、255.255.255.0 というネットワークマスクを使用している場合、サブネットはアドレスの最初の 3オクテットで定義されます。この場合は、192.168.2 です。管理コンピュータのIPアドレスが 192.168.10.5 である場合、同じサブネット上にないため、ゲートウェイが必要になります。ゲートウェイルータは、192.168.2 サブネット上にインタフェースが必要であり、管理コンピュータに連絡できなければなりません。この例では、ゲートウェイの IP アドレスは 192.168.2.1 とします。

13. **警告メッセージを確認してインストールを開始します。**
警告は注意して読んでください。確認後、PC にすでに存在するすべてのデータが削除されます。

インストールをキャンセルしてリブートするには、「*いいえ*」を選択します。

警告 – インストールプロセスを行うと、ハードディスクドライブ上のすべてのデータが削除されます。

ソフトウェアのインストールプロセスには最大2、3分かかる可能性があります。

「*インストール完了*」画面が表示されます。

14. **CD-ROM を取り出して、内部ネットワークに接続し、システムをリブートします。**
インストールプロセスが完了したら、ドライブから CD-ROM を取り出して、`eth0` ネットワークカードを内部ネットワークに接続します。内部ネットワークカード (`eth0`) を除き、ネットワークカードの順序は、通常 PCI ID およびカーネルドライバによって決定されます。ハードウェア構成を変更すると (特にネットワークカードを取り外した場合や追加した場合など)、ネットワードカード名の順序も変わる可能性があります。

次に、インストール画面で Enter を押し、UTMをリブートします。ブートプロセス中に、内部ネットワークカードの IP アドレスが変わります。このとき、インストールルーチンコンソール (Alt+F1) に、「eth0 に IP なし (No IP on eth0)」というメッセージが表示されます。

Sophos UTMのリブート後 (ハードウェアによっては、このプロセスは数分かかります)、`eth0` インタフェースの IP アドレスを ping し、このアドレスが到達可能であることを確認します。接続できない場合、次のいずれかの問題が発生していないかチェックしてください。

- Sophos UTMの IP アドレスが誤っている。
- 管理者コンピュータの IP アドレスが正しくない。
- クライアントのデフォルトゲートウェイが正しくない。
- 正しくないネットワークカードにネットワークケーブルが接続されている。
- すべてのネットワークカードが同じハブに接続されている。

1.4 基本設定

インストールの 2番目のステップは WebAdmin で行います。これは、Web ベースのSophos UTM管理インタフェースです。基本システム設定の前に、Sophos UTMをネットワークに統合する方法を計画

しておく必要があります。どのような機能を提供するか（ブリッジモードと標準（ルーティング）モードのどちらで運用するか、インタフェース間でデータパケットの流れをどのようにコントロールするかなど）を決定する必要があります。ただし、Sophos UTMは後でいつでも再設定できます。したがって、Sophos UTMをネットワークに統合する方法をまだ計画していない場合でも、すぐに基本設定に着手することも可能です。

1. **ブラウザを起動して、WebAdminを開きます。**
   Sophos UTMの URLSophos UTM（eth0 の IP アドレスなど）を参照します。上記の設定例との整合性を保つために、これは `https://192.168.2.100:4444` とします（プロトコルが HTTPSであり、ポート番号が 4444 であることに注意してください）。

   設定例と異なり、各Sophos UTMの出荷時は次のデフォルト設定になっています。

   - **インタフェース:**内部ネットワークインタフェース（eth0）
   - **IP アドレス:**192.168.0.1
   - **ネットワークマスク:**255.255.255.0
   - **デフォルトゲートウェイ:**なし

   任意のSophos UTMの WebAdmin にアクセスするには、代わりに次の URL を入力します。

   `https://192.168.0.1:4444`

   認証および暗号化された通信を提供するために、Sophos UTMには、自己署名済みのセキュリティ証明書が含まれています。この証明書は、WebAdmin への HTTPS 接続が確立するとWeb ブラウザに対して提示されます。証明書の有効期間を確認できない場合、ブラウザはセキュリティ警告を表示します。証明書に同意すると、最初のログインページが表示されます。

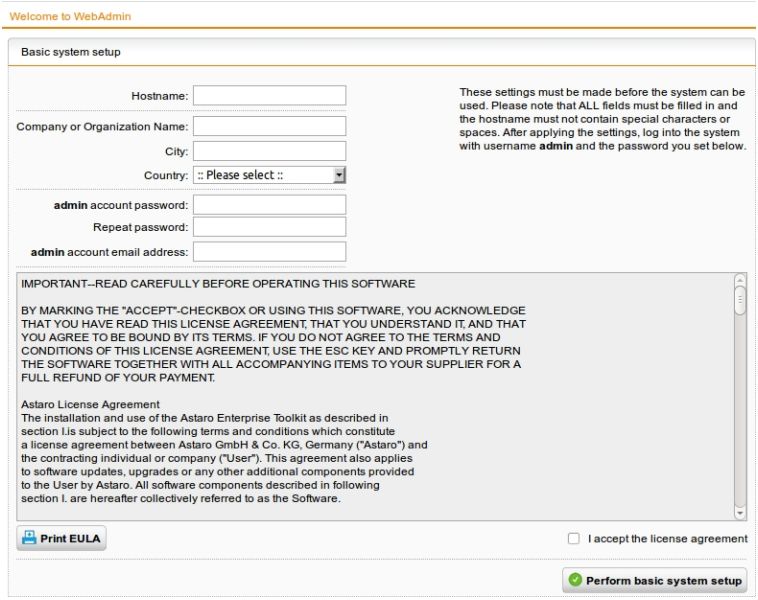

Figure 1 WebAdmin:初期ログインページ

2. **「基本システム設定」フォームに必要事項を入力します。**
   ここに表示されるテキストボックスに会社の情報を正確に入力します。さらに、管理者アカウントのパスワードと有効なメールアドレスを指定します。ライセンス条件に同意する場合は、「*基本システム設定の実行*」ボタンをクリックしてログインを続行します。基本システム設定の実行中、多数の証明書と認証局が作成されます。

   - **WebAdmin CA:**WebAdmin 証明書が署名された CA(「*マネジメント > WebAdmin の設定 > HTTPS 証明書*」を参照)。
   - **VPN に署名する CA:**VPN 接続に使用されるデジタル証明書に署名する CA(「*サイト間 VPN > 認証管理 > 認証局*」を参照)。
   - **WebAdmin 証明書:**WebAdmin のデジタル証明書(「*サイト間 VPN > 証明書管理 > 証明書*」を参照)。
   - **ローカル X.509 証明書:**VPN 接続に使用される、Sophos UTMのデジタル証明書(「*サイト間 VPN > 証明書管理 > 証明書*」を参照)。

   ログインページが表示されます。(ただし、入力した値に基づいて証明書が変更されているため、一部のブラウザでは、さらにセキュリティ警告が表示される場合もあります。)

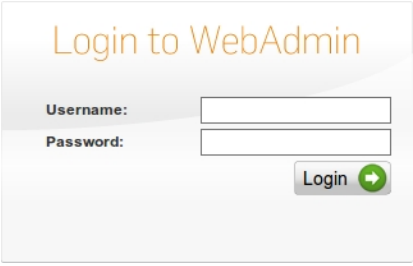

Figure 2 WebAdmin:通常のログインページ

3. **WebAdmin にログインします。**
「ユーザ名」フィールドに「admin」と入力し、前の画面で指定したパスワードを入力します。

   初期設定プロセスをガイドする設定ウィザードが表示されます。ウィザードのステップに従い、Sophos UTMの基本設定を行います。

   バックアップファイルがある場合、代わりにこのバックアップファイルをリストアすることもできます(「バックアップリストア」のセクションを参照)。

   あるいは、(ウィザードの任意のステップで)「キャンセル」をクリックし、安全にウィザードを終了することもできます(Sophos UTMを WebAdmin で直接設定したい場合など)。どの段階でも「終了」をクリックし、そこまでの設定を保存してウィザードを終了できます。

4. **ライセンスをインストールします。**
購入したライセンス(テキストファイル)をアップロードするには、フォルダのアイコンをクリックします。「次へ」をクリックしてライセンスをインストールします。ライセンスを購入していない場合、「次へ」をクリックして、製品に組み込まれた 30日間のトライアルライセンスを使用してください。Sophos UTMに搭載されたすべての機能が有効になります。

5. **内部ネットワークインタフェースを設定します。**
内部ネットワークインタフェース(*eth0*)に対して表示された設定を確認します。このインタフェースの設定は、ソフトウェアのインストール時に提供した情報に基づいています。さらに、チェックボックスにチェックを入れて、Sophos UTMが内部インタフェースで DHCP サーバとして機能するように設定することができます。

   注 – 内部インタフェースの IP アドレスを変更する場合、ウィザード終了後に新しい IP アドレスを使用して WebAdmin に接続し直す必要があります。

6. **外部インタフェースのアップリンクタイプを選択します。**
   外部ネットワークカードで使用するアップリンク/インターネット接続の接続タイプを選択します。インタフェースのタイプとその設定は、どのような種類のインターネット接続を使用するかによって異なります。「*次へ*」をクリックします。

   Sophos UTMにアップリンクがないか、今すぐ設定したくない場合には、「*インターネットアップリンクタイプ*」入力ボックスを空欄のまま残します。インターネットアップリンクを設定すると、内部ネットワークからインターネットへの接続用にIPマスカレードが自動設定されます。

   「*スタティックIP アドレスによる標準イーサネットインタフェース*」を選択する場合、「*デフォルトゲートウェイ*」の指定はオプションです。テキストボックスを空欄のままにすると、インストール時の デフォルトゲートウェイ設定が維持されます。「*次へ*」をクリックして、残りの各ステップをスキップすることができます。スキップした設定は、後でWebAdminで設定・変更できます。

7. **基本的なファイアウォール設定を行います。**
   ここで、インターネットで許可するサービスのタイプを選択できます。「*次へ*」をクリックして設定を確認します。

8. **基本的な侵入防御(IPS)設定を行います。**
   ここで、複数のオペレーションシステムとデータベースに対する侵入防御を設定できます。「*次へ*」をクリックして設定を確認します。

9. **アプリケーションコントロールとネットワーク可視化の設定を行います。**
   ネットワーク可視化を有効にする場合は、ここで選択できます。「*次へ*」をクリックして設定を確認します。

10. **Webプロテクション設定を行います。**
    ここで、Webトラフィックに対してウイルスやスパイウェアのスキャンを行うかどうかを選択できます。さらに、特定のカテゴリに属するWebページのブロックを選択できます。「*次へ*」をクリックして設定を確認します。

11. **メールプロテクション設定を行います。**
    ここでは、最初のチェックボックスにチェックを入れて、POP3プロキシを有効にすることができます。ここでは、2つ目のチェックボックスにチェックを入れて、UTMをインバウンド SMTP リレーとして有効にすることができます。内部メールサーバの IP アドレスを入力し、SMTP ドメインをルートに追加します。「*次へ*」をクリックして設定を確認します。

12. **設定を確認します。**
    設定のサマリが表示されます。「*終了*」をクリックして確認するか、「*戻る*」をクリックして変更します。これらは後でWebAdminで変更することもできます。

「終了」をクリックすると設定は保存され、ユーザは WebAdmin のダッシュボードにリダイレクトされます。ここには、Sophos UTMユニットの最も重要なシステムステータス情報が表示されます。

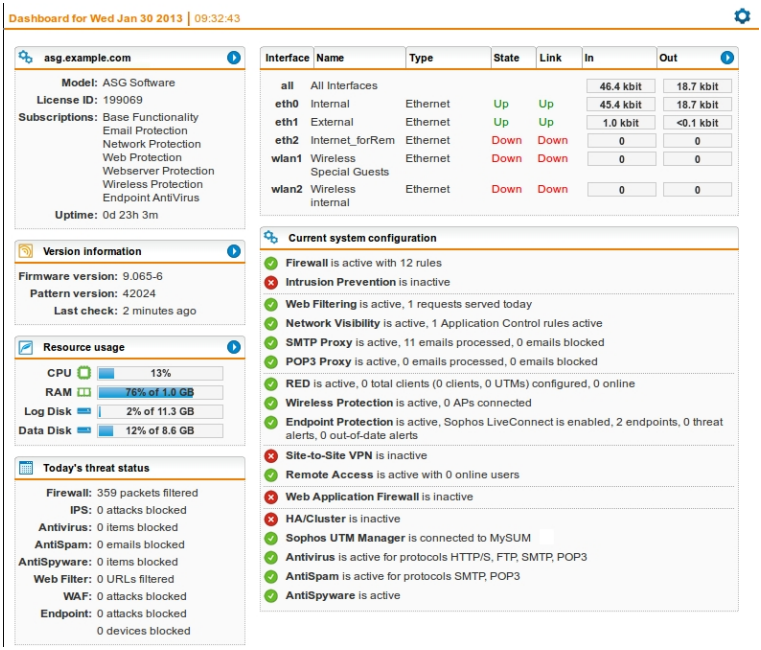

Figure 3 WebAdmin:ダッシュボード

これらのステップの実行中に問題が発生した場合は、Sophos UTMサプライヤのサポート部門にお問い合わせください。次の Web サイトでも詳細情報を提供しています。

- Sophos UTM サポートフォーラム
- Sophos サポートデータベース

1.5 バックアップリストア

WebAdmin 設定ウィザード（「基本設定」のセクションを参照）を使用すると、基本設定プロセスをすべて実行する代わりに、既存のバックアップファイルをリストアすることができます。以下の手順に従ってください。

1. **設定ウィザードで「*既存のバックアップファイルのリストア*」を選択します。**
   設定ウィザードで「*既存のバックアップファイルのリストア*」を選択し、「*次へ*」をクリックします。

   アップロードページが表示されます。

2. **バックアップをアップロードします。**
   フォルダアイコンをクリックし、リストアするバックアップファイルを選択して、「*アップロード開始*」をクリックします。

3. **バックアップをリストアします。**
   「*終了*」をクリックしてバックアップをリストアします。

重要 – 後で設定ウィザードを使用することはできません。

バックアップのリストアが成功すると、ログインページにリダイレクトされます。

2 WebAdmin

WebAdmin は Web ベースの管理インタフェースで、ここではSophos UTMのあらゆる局面の設定を行うことができます。WebAdmin はメニューとページで構成され、それらの多くには複数のタブが含まれています。画面左側のメニューには、Sophos UTMの機能が論理的に構成されています。「*Network Protection*」などのメニュー項目を選択すると、それが拡大してサブメニューが表示されたり関連ページが開きます。メニュー項目の中には、関連ページがないものもあります。前に選択したメニューまたはサブメニュー項目のページは、そのまま表示されます。サブメニュー項目のいずれかを選択すると、それによって最初のタブの関連ページが開きます。

このドキュメントの手順に従ってメニュー項目、サブメニュー項目、およびタブを指定するとページが開きます。例:「*インタフェースとルーティング* > *インタフェース* > *ハードウェア*」タブで、... を設定します ...

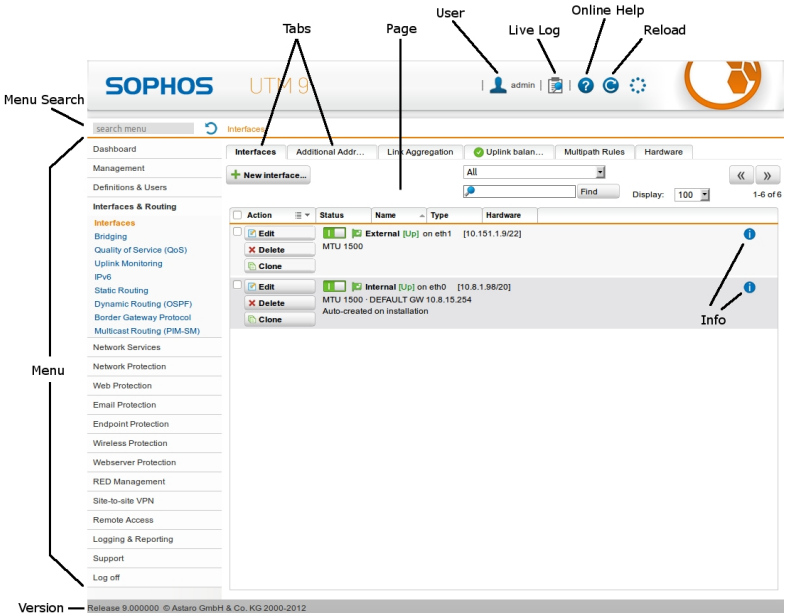

Figure 4 WebAdmin:概要

2.1 WebAdmin メニュー

WebAdmin メニューは、Sophos UTMのすべての設定オプションへのアクセスを提供します。したがって、特定パラメータの設定にコマンドラインインタフェースを使用する必要はありません。

- **ダッシュボード:**ダッシュボードは、Sophos UTM ユニットの現在の操作状況をグラフィカルに表示します。
- **管理:**基本的なシステム設定、WebAdmin 設定、およびユニットの設定に関するすべての設定を構成します。
- **定義とユーザ:**Sophos UTM ユニットで使用するネットワーク、サービス、時間帯定義、およびユーザアカウント、ユーザグループ、外部認証サーバを構成します。
- **インタフェースとルーティング:**ネットワークインタフェースおよびルーティングオプションなどのシステム機能を設定します。
- **ネットワークサービス:**DNS や DHCP などのネットワークサービスを設定します。
- **ネットワークプロテクション:**ファイアウォールルール、VoIP、侵入防御設定などの基本的なネットワークプロテクション機能を設定します。
- **Webプロテクション:**Sophos UTM ユニットの Web フィルタおよびアプリケーションコントロール、ならびに FTP プロキシを設定します。
- **Eメールプロテクション:**Sophos UTM ユニットの SMTP および POP3 プロキシ、さらにメール暗号化を設定します。
- **エンドポイントプロテクション:**ネットワーク上のエンドポイントデバイスの保護を設定・管理します。
- **ワイヤレスプロテクション:**ゲートウェイのワイヤレスアクセスポイントを設定します。
- **Webサーバプロテクション:**Web サーバをクロスサイトスクリプティングや SQL インジェクションなどの攻撃から防御します。
- **REDマネジメント:**RED (Remote Ethernet Device) アプライアンスを設定します。
- **サイト間 VPN:**サイト間 VPN (バーチャル プライベート ネットワーク) を設定します。
- **リモートアクセス:**Sophos UTM ユニットへのリモートアクセス VPN 接続を設定します。
- **ログとレポート:**Sophos UTM ユニットの使用状況に関するログメッセージと統計を表示し、ログおよびレポーティングに関する設定を構成します。

- **サポート:**Sophos UTM ユニットで利用できるサポートツールにアクセスします。
- **ログオフ:**ユーザインタフェースからログアウトします。

メニューの検索

メニュー上部に検索ボックスがあります。ここではキーワードについてメニューを検索し、特定のトピックに関するメニューを容易に検索できます。検索機能はメニュー名を検索しますが、非表示の索引付けされた別名やキーワードも検索できます。

検索ボックスに入力を開始するとすぐに、関連するメニュー項目のみが自動的に表示されます。検索ボックスはそのままにして、該当すると予想されるメニュー項目をクリックしてください。少なくなったメニュー項目はそのまま残り、その隣りのリセットボタンをクリックするまで検索結果が表示されます。

ヒント – キーボードショートカット `CTRL+Y` で検索ボックスにフォーカスすることができます。

2.2 ボタンバー

WebAdmin の右上隅にあるボタンから、次の機能にアクセスできます。

- **ユーザ名/IP:**現在ログインしているユーザと、WebAdmin にアクセスしている IP アドレスを示します。現在他のユーザもログインしている場合は、他のユーザのデータも表示されます。
- **ライブログを開く:**このボタンをクリックすると、現在使用している WebAdmin メニューまたはタブに関連するライブログが開きます。メニューまたはタブを変更しなくても他のライブログを表示するには、ライブログ (Live Log) ボタンの上にカーソルを合わせます。数秒後に使用可能なすべてのライブログのリストが表示されるため、ここで表示するライブログを選択できます。この選択は、同じ WebAdmin メニューまたはタブを使用する限り、記憶されます。

  ヒント – 多くの WebAdmin ページに用意された「*ライブログを開く*」ボタンをクリックしてもライブログを開くことができます。

- **オンラインヘルプ:**すべてのメニュー、サブメニュー、タブにはオンラインヘルプ画面があり、WebAdmin の現在ページのコントロールに関連するコンテキストに応じた情報や手順を提供します。

> **注**– オンラインヘルプはバージョンに基づいており、パターンによって更新されます。新しいファームウェアバージョンに更新したときに、オンラインヘルプの更新が利用できる場合は、オンラインヘルプも更新されます。

- **リロード**:すでに表示されている WebAdmin ページを再び要求する場合、必ず「*リロード*」ボタンをクリックしてください。

> **注** – ブラウザの「再読み込み」ボタンや「更新」ボタンは使用しないでください。これを行うと、WebAdmin からログアウトすることになります。

2.3 リスト

WebAdmin の多くのページにはリストがあります。各リストの左にあるボタンを使用すると、アイテムの編集、削除、または複製が可能です(詳しくは「*ボタンとアイコン*」セクションを参照してください)。リストにアイテムを追加するには、「*新規...*」ボタンをクリックします。ここで「...」は、作成中のオブジェクト(インタフェースなど)を示すプレースホルダです。ダイアログボックスが開き、新規オブジェクトのプロパティを定義することができます。

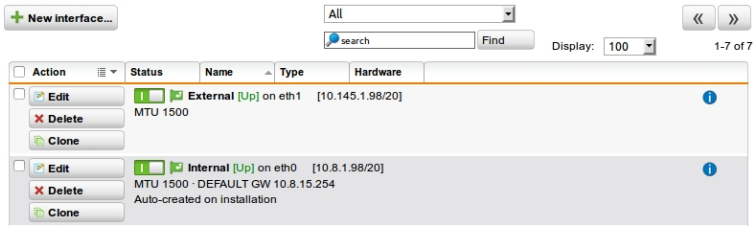

Figure 5 WebAdmin:リストの例

上部のドロップダウンリストを使用して、タイプやグループごとにアイテムをフィルタリング表示できます。上部にある2つ目のフィールドでは、具体的なアイテムを検索することができます。検索文字列を入力し、「*検索*」をクリックします。

アイテムが 11個以上含まれるリストは、複数ページに分割され、「>」(次へ)ボタンと「<」(前へ)ボタンを使用して移動することができます。ただし、この設定は「*ユーザ設定*」タブで変更できます。

リストのヘッダには、機能があります。通常、ヘッダフィールドをクリックすると、その名前のそのオブジェクトフィールドによりリストがソートされます。たとえば、「*名前*」フィールドをクリックすると、オブジェクト名によりリストがソートされます。ヘッダの「*アクション*」フィールドには、選択しているリス

トオブジェクトに対して実行できるバッチオプションがあります。オブジェクトを選択するには、チェックボックスにチェックを入れます。この選択は、複数ページにわたって維持されます。つまり、リストを数ページにわたって閲覧する間、既に選択したオブジェクトが選択された状態で維持されます。

ヒント – 情報アイコンをクリックすると、そのオブジェクトが使用されているすべての設定オプションが表示されます。

2.4 リストの検索

フィルタフィールドを使用すると、リストに表示される項目数を制限することができます。これにより、目的のオブジェクトを素早く探すことができます。

重要事項

- リストの検索では、通常複数のフィールドで検索式を検索します。たとえば、「ユーザとグループ」で検索を行うと、ユーザ名、実際の名前、コメント、主要メールアドレスが検索されます。一般的に、情報アイコンを使用して表示される情報を除いて、リストに表示されるすべてのテキストに検索が行われます。
- リストの検索では、大文字と小文字が区別されないため、大文字または小文字のどちらを入力しても同じ結果になります。検索結果には、一致した大文字と小文字のテキストが表示されます。大文字または小文字のテキストを限定して検索することはできません。
- リストの検索は、Perl 正規表現構文に基づいています(しかし、大文字と小文字は区別されません)。テキストエディタなどでよく使用される＊や？などの単純なワイルドカード文字、AND や OR などの演算子をはじめとする検索式は、リスト検索では*機能しません*。

例

ここには、役立つ検索文字列をいくつか示します。

単純な文字列:指定した文字列を含むすべての単語を検索します。たとえば、"inter" を指定すると、"Internet"、"interface"、"printer" が検索されます。

単語の最初:検索文字列の最初に`\b`を付加します。たとえば、`\binter`を指定すると、"Internet" と "interface" が検索されますが、"printer" は検索されません。

単語の最後:検索文字列の最後に\bを付加します。たとえば、http\bを指定すると、"http" が検索されますが、"https" は検索されません。

エントリの最初:検索文字列の最初に ^ を付加します。たとえば、^interを指定すると、"Internet Uplink" が検索されますが、"Uplink Interfaces" は検索されません。

IP アドレス:IP アドレスを検索する場合は、ドットをバックスラッシュでエスケープする必要があります。たとえば、192\.168を指定すると、"192.168" が検索されます。
IP アドレスを一般的に検索するには、\dを使用してあらゆる桁を検索します。\d+を指定すると、行の複数の桁が一致します。たとえば、\d+\.\d+\.\d+\.\d+を指定すると、あらゆるIPv4アドレスが検索されます。

注 – より完全な検索文字列を指定すると、予想しない結果が得られたり、不正確な結論を導くことになるため、それよりは簡単で無難な検索文字列を使用して多くの検索結果を得ることをお勧めします。

正規表現の詳細とSophos UTMでの使用方法については、「Sophos」を参照してください。

2.5 ダイアログボックス

ダイアログボックスとは、特定の情報の入力を求めるためにWebAdminが使用する特別なウィンドウです。例として、「*インタフェース & ルーティング > スタティックルーティング*」メニューで表示される、新しいスタティックルートを作成するためのダイアログボックスを示します。

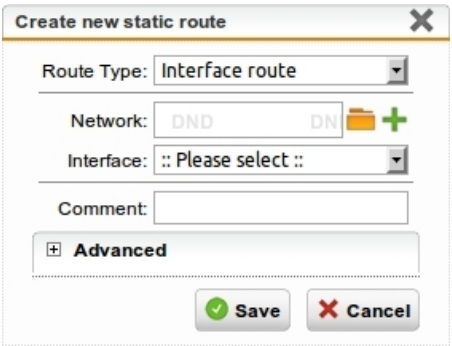

Figure 6 WebAdmin:ダイアログボックスの例

各ダイアログボックスは、テキストボックス、チェックボックスなどの各種ウィジェットから構成されています。さらに、多くのダイアログボックスにはドラッグ & ドロップ機能があり、*DND* と記された特

別な背景で識別されます。このようなボックスが表示された場合、ボックスにオブジェクトをドラッグすることができます。オブジェクトをドラッグする元の場所となるオブジェクトリストを開くには、テキストボックスのすぐ横にある「フォルダ」アイコンをクリックします。これにより、設定オプションに応じて、使用可能なネットワーク、インタフェース、ユーザ/グループ、またはサービスのリストが開きます。緑色の「+」アイコンをクリックすると、新しい定義を作成するためのダイアログボックスが開きます。特定の設定で不要なウィジェットは、グレーアウト表示されます。これらのウィジェットを編集できる場合もありますが、効果はありません。

注 – WebAdmin には、「*保存*」ボタンと「*適用*」ボタンの両方が存在します。「*保存*」ボタンは、スタティックルートやネットワーク定義といった WebAdmin 内のオブジェクトを作成または編集するときに使用します。常に、対応する「*キャンセル*」ボタンが用意されています。一方、「*適用*」ボタンは、バックエンドで設定を確認し、速やかに有効にするために使用します。

2.6 ボタンとアイコン

ここでは、WebAdmin で使用されているボタンとアイコンの用途について説明します。

ボタン	意味
View	オブジェクトの詳細情報を示すダイアログウィンドウが表示されます。
Edit	オブジェクトのプロパティを編集するためのダイアログウィンドウが開きます。
Delete	オブジェクトを削除します。そのオブジェクトが他の箇所でまだ使用されている場合は、警告が表示されます。使用中のオブジェクトは削除できない場合があります。
Clone	同じ設定やプロパティで別のオブジェクトを作成するためのダイアログウィンドウが開きます。同じ設定を何度も繰り返し入力する必要なく、類似のオブジェクトを作成できます。

機能アイコン	意味
	情報:オブジェクトが使用されているすべての設定が表示されます。
	詳細:このトピックについての詳細な情報は他の 管理ガイド ページにリンクされています。

機能アイコン	意味
	トグルスイッチ:機能を有効または無効にします。有効な場合は緑、無効な場合はグレー、有効化する前に設定が必要な場合はアンバーとなります。
	フォルダ:2種類の機能があります。(1) 左側にあるオブジェクトリストを開く(下のセクションを参照)。ここで適切なオブジェクトを選択できます。(2) ファイルのアップロード用のダイアログウィンドウを開く。
	プラス (+):必要なタイプの新しいオブジェクトを追加するためのウィンドウが開きます。
	アクション:ドロップダウンメニューをこのボタンで開きます。このアイコンはページにより機能は異なります。(1) リストヘッダにある場合、「*有効化*」、「*無効化*」、「*削除*」を選択したオブジェクトに適用。(2) テキストボックスにある場合、「*インポート*」/「*エクスポート*」を使用して、テキストをインポート/エクスポートできます。また、「*空にする*」を使って、コンテンツ全体を削除することもできます。一部の要素にリストを絞るためのフィルタフィールドも提供されています。フィルタでは大文字と小文字が区別されます。
	空にする:オブジェクトの前にある場合、現在の設定からオブジェクトを除去します。「*アクション*」メニューにある場合、ボックスからすべてのオブジェクトを除去します。ただし、このオブジェクトは削除されるわけではありません。
	インポート:複数のアイテムまたは行を持つテキストをインポートするためのダイアログウィンドウが開きます。複数のアイテムを個別に入力するのではなく、まとめて追加することができます(たとえば、URL ブラックリストに大規模なブラックリストを追加する)。任意の場所からテキストをコピーし、CTRL+V で貼り付けます。
	エクスポート:既存のアイテムをすべてエクスポートするためのダイアログウィンドウが開きます。アイテムを区切るための区切り文字として、新しい行、コロン、コンマのいずれかを選択できます。アイテムをテキストとしてエクスポートするには、「*エクスポートするテキスト*」フィールドでテキスト全体を選択し、CTRL+C を押してコピーします。続いて、CTRL+V を使用してすべての共通アプリケーション(テキストエディタなど)にこれを貼り付けます。
	ソート:2つの矢印を使用してリストの各要素を上下に動かし、並べ替えることができます。
	前へ/次へ:ページによっては、2つの矢印を使用して長いリストのページ間の移動や、変更や設定の履歴を前へ(または後ろへ)移動することができます。
	PDF:現在表示されているデータを PDF ファイルに保存してから、保存したファイルをダウンロードするためのダイアログウィンドウが開きます。
	CSV:現在表示されているデータを CSV(コンマ区切り値)ファイルに保存してから、保存したファイルをダウンロードするためのダイアログウィンドウが開きます。

2.7 オブジェクトリスト

オブジェクトリストとは、WebAdmin の左側に一時的に表示されるドラッグ＆ドロップリストで、メインメニューをカバーします。

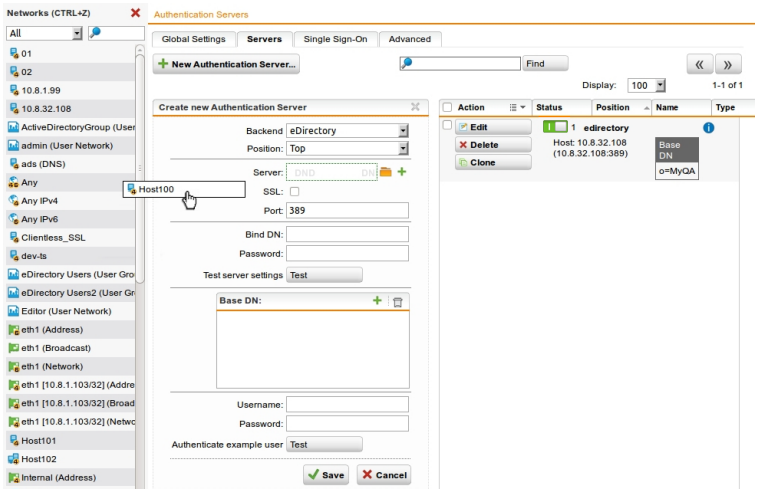

Figure 7 WebAdmin:オブジェクト リスト *ネットワーク*からオブジェクトをドラッグする

オブジェクトリストは、「フォルダ」アイコンをクリックすると自動的に開きます（上のセクションを参照）。あるいは、キーボードショートカットを使用して手動で開くこともできます（「*管理 > WebAdmin 設定 >*ユーザ設定」を参照）。

オブジェクトリストから、ユーザ/グループ、インタフェース、ネットワーク、サービスなどの WebAdmin オブジェクトにすばやくアクセスし、設定時に選択することができます。オブジェクトを選択するには、現在の設定にオブジェクトをドラッグ＆ドロップするだけです。

既存の各種オブジェクトタイプに従い、オブジェクトリストには 5つのタイプがあります。「フォルダ」アイコンをクリックすると、現在の設定で必要なタイプが常に開きます。

3 ダッシュボード

ダッシュボードは、Sophos UTMの現在の操作状況をグラフィカルに表示します。

このダッシュボードにはデフォルトで、ユーザがいつWebAdminにログインしたのかを示す情報と次の情報が表示されます。

ヒント – 右上のダッシュボード設定アイコンをクリックするとダイアログウィンドウが開き、ここでどのトピックセクションを表示するかなどを設定できます。

- **一般情報**:ユニットのホスト名、モデル、ライセンスID、アップタイム。サブスクリプションの表示色は、有効期限が切れる30日前からオレンジ色に変わります。7日前から、また有効期限が切れると、サブスクリプションの表示色は赤になります。
- **バージョン情報**現在インストールされているファームウェアとパターンバージョン、および利用可能な更新パッケージの情報。
- **リソース使用状況**:次のコンポーネントを含むシステムの現在の使用状況。
  - CPU使用率(%)
  - RAM使用率(%)
  - ログパーティションで消費されているハードディスクの容量(%)
  - ルートパーティションで消費されているハードディスクの容量(%)
  - UPS(無停電電源装置)モジュールがある場合はその状況
- **今日の脅威ステータス**:深夜以降に検出された関連するセキュリティ脅威のカウンタ:
  - ログが有効になっているドロップされたデータパケットと拒否されたデータパケットの合計
  - 侵入がブロックされた回数の合計
  - ブロックされたウイルスの合計(全プロキシ)
  - ブロックされたスパムメッセージの合計(SMTP/POP3)
  - ブロックされたスパイウェアの合計(全プロキシ)
  - ブロックされたURLの合計(HTTP/S)
  - ブロックされたWebサーバ攻撃の合計(WAF)

- **インタフェース:**設定されているネットワークインタフェースカードの名前とステータス。さらに、受信トラフィックと送信トラフィックの両方に対する過去 75秒間の平均ビットレートに関する情報も表示されます。表示される値は、15秒間隔で収集されるサンプルに基づく平均ビットレートから取得されます。インタフェースのトラフィックアイコンをクリックすると、フローモニタが新しいウィンドウで開きます。フローモニタには、過去10分間のトラフィックが表示され、短い間隔で自動更新されます。フローモニタについて詳しくは、「フローモニタ」を参照してください。
- **現在のシステム設定:**関連セキュリティ機能が有効であるか無効であるかを示します。エントリをクリックするとWebAdmin page が開き、各設定が表示されます。
  - **ファイアウォール:**アクティブファイアウォールルールの合計に関する情報。
  - **IPS:**侵入防御システム(IPS)は、シグニチャに基づくIPS ルールセットを利用して攻撃を認識します。
  - **Web フィルタリング:**HTTP/S プロトコル用のアプリケーションレベルのゲートウェイ。サービスの使用が許可されているネットワークに対し、豊富な Web フィルタ技術を提供します。
  - **ネットワークの可視化:**SophosSophos のレイヤ7アプリケーションコントロールを使用すると、ネットワークトラフィックを分類およびコントロールできます。
  - **SMTP プロキシ:**SMTP *(簡易メール転送プロトコル)*を使用したメッセージ送信用のアプリケーションレベルのゲートウェイ。
  - **POP3 プロキシ:**POP3 *(Post Office Protocol 3)*を使用したメッセージ送信用のアプリケーションレベルのゲートウェイ。
  - **RED:**支店のセキュリティ用の Remote Ethernet Device(RED)アプライアンスの設定。
  - **ワイヤレスプロテクション:**ワイヤレスネットワークおよびアクセスポイントの設定。
  - **エンドポイントプロテクション:**ネットワーク上のエンドポイント端末の管理。接続中のエンドポイントの数や警告を表示します。
  - **サイト間 VPN:**サイト間 VPN シナリオの設定。
  - **リモートアクセス:**ロードウォリア VPN シナリオの設定。
  - **WAF:**Web サーバをクロスサイトスクリプティングや SQL インジェクションなどの攻撃から防御するためのアプリケーションレベルのゲートウェイ。
  - **HA/クラスタ:**冗長化(HA)フェイルオーバーおよびクラスタリング。つまり、処理集約型のタスク(コンテンツフィルタ、ウイルススキャン、侵入検知、復号化など)を複数のクラスタノードに均一に分散します。

- **Sophos UTM Manager:**集中管理ツール Sophos UTM Manager (SUM) 経由での Sophos UTM アプライアンスの管理。
- **ウイルス対策:**ウイルス、ワーム、その他のマルウェアなどの有害で危険なコンテンツを伝送する Web トラフィックからネットワークを保護します。
- **スパム対策:**未承諾のスパムメールを検知し、既知の (または疑わしい) スパム発信者からのスパム送信を特定します。
- **スパイウェア対策:**シグニチャデータベースとスパイウェアフィルタリング技術が定期的に更新される 2種類のウイルススキャンエンジンを使用して、スパイウェア感染を防止します。受信トラフィックと送信トラフィックの両方を保護します。

3.1 ダッシュボード設定

ダッシュボードでは、いくつかの設定を変更できます。ダッシュボード右上のダッシュボード設定アイコンをクリックすると「*ダッシュボード設定の編集*」ダイアログウィンドウが開きます。

ダッシュボードの更新:デフォルトで、ダッシュボードは 5秒間隔で更新されます。更新間隔は「*無し*」～「*60秒*」の間で設定できます。

左の列 – 右の列:ダッシュボードは、各トピックに関する情報を示すいくつかのトピックセクションに分かれています。「*左の列*」および「*右の列*」の 2つのボックスを使用すると、これらのトピックセクションの配置を変えたり、表示に追加したり表示から削除することができます。これらの設定がその後ダッシュボードに反映されます。列のトピックセクションを並べ替えるには、矢印アイコンを使用します。特定のトピックセクションを表示に追加したり表示から削除するには、チェックボックスにチェックを入れるか、外します。

デフォルトで表示されるトピックセクションについては、「ダッシュボード」の章を参照してください。追加のトピックセクションも表示することができ、ここでそれについて説明します。

- **Web プロテクション:上位アプリケーション:**最もよく使用されているアプリケーションの概要。このセクションでは、アプリケーション名の上にカーソルを合わせると、追加機能が 1つまたは 2つ表示されます。
  - *Block* アイコンをクリックすると、現時点から該当アプリケーションがブロックされます。これにより、「*アプリケーション コントロール*」ページにルールが作成されます。このオプションは、Sophos UTMの正常なオペレーションに必要なアプリケーションに対しては利用できません。たとえば、WebAdmin トラフィックはブロックできません。これをブロックすると、ユーザ自身が WebAdmin からシャットアウトされてしまいます。未分類のトラフィックもブロックできません。

- *Shape* アイコンをクリックすると、当該アプリケーションのトラフィックシェーピングが有効になります。ダイアログウィンドウが開き、ルール設定を定義するよう要求されます。完了したら「*保存*」をクリックします。これにより、「*トラフィックセレクタ*」および「*帯域幅プール*」ページにルールが作成されます。
  シェーピングはインタフェース単位で機能するため、「*すべてのインタフェース*」フローモニタを閲覧している際はトラフィックシェーピングを利用できません。

- **Web プロテクション:Top サイト時間別:**最もよく閲覧されたドメインの時間別の概要。
- **Web プロテクション:トラフィックの多いサイト:**最もよく閲覧されたドメインのトラフィック別の概要。
- **ログ:**ディスクの残容量、フィルアップレート（使用量増加速度）の情報を含む Sophos UTM ユニットのログパーティションのステータス。
- **ニュースフィード:**Sophos およびその製品に関するニュース。
- **グラフ:同時接続数:**同時接続の総数に関する日々の統計およびヒストグラム。
- **グラフ:ログパーティション ステータス:**ログパーティションの使用状況に関する過去 4週間の統計およびヒストグラム。
- **グラフ:CPU 使用率:**現在のプロセッサ使用状況 (%) に関する日々の統計およびヒストグラム。
- **グラフ:メモリ/スワップの使用状況:**メモリおよびスワップの使用状況 (%) に関する日々の統計およびヒストグラム。
- **グラフ:パーティションの使用状況:**選択したパーティションの使用状況 (%) に関する日々の統計およびヒストグラム。

ダッシュボードでの自動グループ化の有効化:ダッシュボード上にコンパクトに情報を表示するにはこのオプションを選択します。このオプションは、左の列の「*Web プロテクション*」の選択項目と、右の列の「グラフ」の選択項目のみに影響を及ぼします。これを選択すると、各情報要素がダッシュボード上のタブとして重なって表示されます。選択を解除すると、情報要素が左右に並んで表示されます。

「*保存*」をクリックして設定を保存します。

3.2 フローモニタ

Sophos UTMのフローモニタは、現在UTMのインタフェースを通過しているネットワークトラフィックに関する情報を素早く確認するためのアプリケーションです。ダッシュボードの右上でいずれかのインタフェースをクリックすることにより簡単にアクセスできます。「*すべてのインタフェース*」をクリック

すると、すべてのアクティブなインタフェースについて蓄積されたトラフィックがフローモニタに表示されます。単一のインタフェースをクリックすると、そのインタフェースのトラフィックのみがフローモニタに表示されます。

注 – フローモニタは新しいブラウザウィンドウで開きます。このウィンドウはポップアップブロッカによってブロックされる可能性があるため、WebAdmin に対してポップアップブロッカを無効にすることをお勧めします。

フローモニタには、チャート（Chart）とテーブル（Tabular）という2種類のビューがあります。それぞれについては後述します。ビューは 5秒間隔で更新されます。更新を停止するには「*一時停止*」ボタンをクリックします。「*続行*」をクリックして更新を再開すると、フローモニタが最新のトラフィック情報に更新します。

チャートビュー

フローモニタのチャートには、過去 10分間のネットワークトラフィックが表示されます。横軸は時間を、縦軸はスループットにスケールを動的に適用したときのトラフィック量を示します。

チャートビューの下部には、インタフェースを通過するトラフィックの種類を示す凡例が表示されます。トラフィックは種類ごとに色分けされるため、チャート内で簡単に見分けることができます。

注 – ネットワーク可視化を有効にした場合（「*Web プロテクション > アプリケーションコントロール > ネットワーク可視化*」の章を参照）、フローモニタはトラフィックについてより差別化された情報を表示します。

マウスのカーソルをグラフ上に置くと、大きなドット（点）が表示され、グラフのその部分の詳細な情報が表示されます。このドットは、グラフの線に沿って移動します。マウスのカーソルを移動すると、ドットもそれに従って移動します。グラフに何本かの線がある場合、ドットはマウスカーソルの移動に従って線の間を移動します。さらに、ドットの色は、それが表示している情報がどの線に関連するかによって変わるため、線が互いに近接している場合に役立ちます。ドットは、ある時点でのトラフィックの種類とサイズに関する情報を示します。

テーブルビュー

フローモニタのテーブルには、過去 5秒間のネットワークトラフィックに関する情報が表示されます。

#:トラフィックは、現在の帯域幅使用状況に基づいてランク付けされます。

Application(アプリケーション):利用可能な場合、ネットワークトラフィックのプロトコルまたは名前。未分類のトラフィックは、システムにとって不明な種類のトラフィックです。アプリケーションをクリックすると、ウィンドウにサーバ、使用ポート、サーバ接続ごとの帯域幅の使用状況、合計トラフィックの情報が表示されます。

Client(クライアント):アプリケーションを使用しているクライアント接続数。クライアントをクリックすると、ウィンドウにクライアントの IP アドレス、クライアント接続ごとに使用される帯域幅、合計トラフィックの情報が表示されます。未分類のトラフィックの場合は、テーブル内のクライアント数が追加情報ウィンドウに表示されるクライアント数よりも多くなる可能性があります。これは「未分類」に複数のアプリケーションが含まれるためです。したがって、情報ウィンドウのクライアント数が 1つでもテーブルには 3つのクライアントが存在する場合があります。これは、1つのクライアントが 3種類の未分類のアプリケーションに接続していることが考えられます。

Bandwidth Usage now(現在の帯域幅使用状況):過去 5秒間の帯域幅使用状況。帯域幅をクリックすると、ウィンドウにアプリケーション接続のダウンロード速度とアップロード速度の情報が表示されます。

Total Traffic(合計トラフィック):接続の「ライフタイム」中に生成されたネットワークトラフィックの合計数。例 1:ダウンロードが、過去のある時点で開始され、まだ継続中です。ダウンロード開始時点から、期間中に生成されたトラフィック全体が表示されます。例 2:複数のクライアントが Facebook を使用しています。いずれか 1つのクライアントが接続をオープンにしている限り、すべてのクライアントによってこれまでに生成されたトラフィックがすべて蓄積されて合計トラフィックに表示されます。
合計トラフィックをクリックすると、ウィンドウにアプリケーション接続の総合ダウンロード速度とアップロード速度の情報が表示されます。

Actions(アクション):アプリケーションの種類に応じて、利用可能なアクションがあります(未分類のトラフィックを除く)。

- ブロック:*Block* ボタンをクリックすると、現時点から該当アプリケーションがブロックされます。これにより、「*アプリケーション コントロール*」ページにルールが作成されます。このオプションは、Sophos UTMの正常なオペレーションに必要なアプリケーションに対しては利用できません。たとえば、WebAdminトラフィックはブロックできません。これをブロックすると、ユーザ自身が WebAdmin からシャットアウトされてしまいます。未分類のトラフィックもブロックできません。
- トラフィックシェーピング:*Shape* ボタンをクリックすると、当該アプリケーションのトラフィックシェーピングが有効になります。ダイアログウィンドウが開き、ルール設定を定義するよう要求されます。完了したら「*保存*」をクリックします。これにより、「*トラフィックセレクタ*」および「*帯域幅プール*」ページにルールが作成されます。

シェーピングはインタフェース単位で機能するため、「*すべてのインタフェース*」フローモニタを閲覧している際はトラフィックシェーピングを利用できません。

- ダウンロード帯域幅調整:*Throttle*ボタンをクリックすると、当該アプリケーションのダウンロード帯域幅の調整が有効になります。ダイアログウィンドウが開き、ルール設定を定義するよう要求されます。完了したら「*保存*」をクリックします。これにより、「*トラフィックセレクタ*」および「*ダウンロード帯域幅調整*」ページにルールが作成されます。ダウンロード帯域幅調整はインタフェース単位で機能するため、*すべてのインタフェース*フローモニタを閲覧している際はダウンロード帯域幅調整を利用できません。

4 マネジメント

この章では、基本システム設定や、Sophos UTM、*WebAdmin*などの Web ベース管理インタフェースの設定を定義する方法を説明します。「*概要*」ページには、加えられた可能性のある変更を含め、最近の WebAdmin セッションの統計が表示されます。変更の詳細を確認するには、「*変更ログ*」列の「*表示*」ボタンをクリックします。

「*状態*」列には、前回の WebAdmin セッションの終了時間が表示されます。

注 – WebAdmin のセッションを終了するには、「*ログオフ*」メニューをクリックします。「*ログオフ*」メニューをクリックしないでブラウザを閉じた場合、「*マネジメント*」>「*WebAdmin 設定*」>「*詳細*」タブで定義した時間が経過すると、セッションはタイムアウトとなります。

この章では、次のトピックについて説明します。

- システム設定
- WebAdmin設定
- ライセンス
- Up2Date
- バックアップ/リストア
- ユーザポータル
- 通知
- カスタマイズ
- SNMP
- 集中管理(SUM)
- 冗長化 (HA)
- シャットダウン/リスタート

4.1 システム設定

「システム設定」の下にあるタブで、ホスト名、日付、時刻など、UTM の基本設定を行うことができます。

4.1.1 組織

組織の名前と所在地、および Sophos UTM の運用を技術的に担当する担当者または担当部署のメールアドレスを入力します。このデータは、IPsec、メール暗号化、および WebAdmin の証明書でも使用されます。

4.1.2 ホスト名

このフィールドにUTM のホスト名を*完全修飾ドメイン名*（FQDN）で入力します（例: `utm.example.com`）。ホスト名には英数字、ドット、およびハイフンを使用できます。ホスト名の末尾には`com`、`org`、`de`などの特殊な識別子を使用する必要があります。ホスト名は、通知メッセージでUTMを識別するために使用されます。また、Web フィルタから送信されたステータスメッセージにも表示されます。お客様のドメインの DNS ゾーンにホスト名を登録する必要はありません。

4.1.3 日付と時刻

UTMでは、日付と時刻を常に正しく設定しておく必要があります。これは、ログおよびレポーティングシステムから正しい情報を取得したり、インターネット上の他のコンピュータとの相互運用性を保証するために必要です。

通常は、日付と時刻を手動で設定する必要はありません。デフォルトで、パブリックのインターネットサーバとの自動同期が有効化されています（「*インターネットサーバと時間を同期*」のセクションを参照）。

まれではありますが、タイムサーバとの同期を無効にする必要がある場合、時刻と日付を手動で変更することができます。ただし、これを行う場合は、以下の警告に注意してください。

- システム時間を標準時間からサマータイムに（あるいはその逆に）変更しないでください。この変更は、タイムサーバとの自動同期を無効にした場合でも、タイムゾーンの設定によって自動的に行われます。
- タイムサーバとの同期が有効になっている場合は、日付または時刻を手動で変更しないでください。多くの場合、自動同期により、手動で行った変更がすぐに取り消されます。日付または時刻を手動で設定する必要がある場合、最初に「*NTP サーバ*」ボックス（下の「*インターネットサーバと時間を同期*」セクション）からすべてのサーバを削除し、「*適用*」をクリックしてください。
- システム時間を手動で変更してから、変更が成功したことを通知する緑色の確認メッセージが表示されるまで待機します。次に、システムをリブートします（「*マネジメント > シャットダ*

ウン/リスタート」)。多くのサービスでは、時間は連続的に変化し、急に変化する訳ではないという事実に依存しているため、これが推奨されます。時間に飛びがあると、様々なサービスの誤作動につながる可能性があります。このアドバイスは、あらゆる種類のコンピュータシステムに共通して該当します。

- まれに、システム時間を変更すると、WebAdmin セッションが強制終了される可能性があります。これが発生した場合、ログインし直して、時刻が正しく設定されていることを確認し、後でシステムを再起動してください。

いくつかのタイムゾーンにまたがる相互接続された複数のUTMを運用している場合は、すべてのデバイスに同じタイムゾーンを選択します(例:UTC(協定世界時))。これにより、ログメッセージをより簡単に比較できます。

システム時間を手動で変更すると、システムを正しく再起動した場合でも、複数の副作用が予想されます。

- **時刻を早める**
  - 時刻に基づくレポートの場合、スキップされた時間のデータがなくなります。ほとんどのグラフでは、この期間は、最近記録された値が直線で表示されます。
  - アカウンティングレポートでは、この期間は、すべての変数が 0 で表示されます。
- **時刻を戻す**
  - 時刻に基づくレポートには、該当する期間のログデータがすでに存在します。
  - ほとんどの図は、この期間に記録された値を圧縮して表示します。
  - ダッシュボードで表示される最後のパターンチェックからの経過時間は、たとえ最後のチェックがほんの数分前に行われた場合であっても、値について「なし」と表示します。
  - UTM上で自動的に作成された証明書は、それらの有効期間の開始日付が将来になっている場合は無効になります。
  - アカウンティングレポートは将来の時刻から記録された値を保持します。再度変更を行った時刻になると、アカウンティングデータは再度通常どおりに記述されます。

こうした欠点があるため、システム時間はシステムのセットアップ時に一度だけ設定し、その後は少し調整するだけにするべきです。これは、レポートデータをさらに処理する必要がある場合やデータの精度が重要な場合には、特に言えることです。

日付と時刻の設定

システム時間を手動で設定するには、日付と時刻をそれぞれのドロップダウンリストから選択します。設定を保存するには「*適用*」をクリックします。

タイムゾーンの設定

システムのタイムゾーンを変更するには、ドロップダウンリストから地域またはタイムゾーンを選択します。設定を保存するには「*適用*」をクリックします。

タイムゾーンを変更してもシステム時間は変更されず、影響があるのは、ロギングデータやレポーティングデータなどの出力における時間の表示のみです。これによってサービスを中断することはありませんが、すべてのサービスで新しい時間設定を使用するように、後で再起動することを推奨します。

インターネットサーバと時間を同期

タイムサーバを使用してシステム時刻の同期をとるには、1台以上の NTP サーバを選択します。設定を終了したら「*適用*」をクリックします。

NTP サーバ:デフォルトでは「*NTP Server Pool*」が選択されています。このネットワーク定義は *pool.ntp.org* プロジェクトのパブリックタイムサーバの大きな仮想クラスタにリンクしています。インターネットサービスプロバイダが顧客用に NTP サーバを運用しており、これらのサーバへのアクセス権がある場合、*NTP Server Pool*を削除してプロバイダのサーバを使用することが推奨されます。独自のサーバまたはプロバイダのサーバを選択する場合、複数のサーバを使用すると、精度や信頼性が向上します。3つの独立したサーバを使用すれば、常に十分です。それ以上のサーバを追加しても、さらなる改良はほとんど期待できず、サーバの負荷が増加します。*NTP Server Pool*と独自またはプロバイダのサーバの両方を使用しても、精度や信頼性は向上しないため、使用は推奨されません。

注 – クライアントマシンがこれらの NTP サーバに接続できるようにするには、「*ネットワークサービス > NTP*」ページの許可されているネットワークにこれらのマシンを追加します。

テスト構成サーバ:デバイスから選択された NTP サーバへの接続を確立できることと、NTP サーバが使用可能な時刻データを返すことをテストする際は、このボタンをクリックします。これで、お使いのシステムとサーバ間の時間のオフセットを測定します。お使いのシステムが正しく設定されており、一定時間にわたって安定した状態で動作している場合は、オフセットは一般的に1秒未満になります。

通常、NTP を有効化したり他のサーバを追加した直後は、オフセットがこれより長くなります。時間の飛びを防ぐために、NTP はゆっくりとシステム時間をずらします。やがて、システム時間は時間の飛びなく補正されます。このような状況が発生した場合は、しばらく待機してください。特に、このような場合には、システムを再起動*しないでください*。その代わりに、約 1時間後に再びチェックしてください。オフセットが減少すると、すべてが正しく機能するようになります。

4.1.4 シェルアクセス

セキュアシェル（SSH）はコマンドラインアクセスモードであり、主にUTMへのリモートシェルアクセスを取得するために使用されます。これは通常、より深いレベルのメンテナンスやトラブルシューティングに使用されます。このシェルにアクセスするには、SSH クライアントが必要です。SSHクライアントは一般的に、ほとんどの Linux ディストリビューションに装備されています。

許可ネットワーク

「*許可ネットワーク*」コントロールを使用して、この機能へのアクセスを特定ネットワークのみに制限します。ここにリストされたネットワークは、SSH サービスに接続できます。

認証

このセクションで、SSH アクセスの認証方法とアクセスの厳格さを定義できます。以下の認証方法を利用できます。

- パスワード（デフォルト）
- 公開鍵
- パスワードと公開鍵

「*公開鍵認証*」を使用するには、公開鍵での認証を許可された各ユーザについて、それぞれの公開鍵を「*ログインユーザに承認された鍵*」フィールドにアップロードする必要があります。

root ログイン許可: root ユーザに対して SSH アクセスを許可できます。このオプションを有効にするとセキュリティリスクが高くなるため、デフォルトでは無効になっています。このオプションを有効にすると、ルートユーザは公開鍵を介してログインできます。「*root 用の公開鍵*」フィールドに root ユーザの公開鍵をアップロードします。

設定を保存するには「*適用*」をクリックします。

シェル ユーザ パスワード

デフォルトのシェルアカウント `root`（ルート）および `loginuser`（ログインユーザ）用のパスワードを入力します。これら 2つのアカウントのいずれか一方のパスワードのみを変更するには、他方のアカウントの入力ボックスを空白のままにします。

注 – SSH シェルアクセスを有効にするには、最初にパスワードを設定する必要があります。さらに、「*定義とユーザ > 認証サーバ > 詳細*」タブで設定したパスワードの複雑さの設定に準拠した

パスワードのみを指定できます。つまり、複雑なパスワードを有効にした場合は、シェルユーザのパスワードも同じ要件を満たすことが必要になります。

SSH デーモンリスニングポート

このオプションで、SSH に使用する TCP ポートを変更できます。デフォルトでは、標準 SSH ポートの 22 が設定されています。ポートを変更するには、1024～65535の適切な値を「*ポート番号*」ボックスに入力し、「*適用*」をクリックします。

4.1.5 スキャン設定

アンチウイルスエンジン設定

WebAdmin を通してすべてのシングルスキャン設定に使用するアンチウイルスエンジンを選択します。デュアルスキャン設定では、両方のアンチウイルスエンジンが使用されます。Basic Guad サブスクリプションではデュアルスキャンは利用できません。設定を保存するには「*適用*」をクリックします。

4.1.6 設定またはパスワードのリセット

「*設定またはパスワードのリセット*」タブのオプションで、シェルユーザのパスワードを削除できます。さらに、工場出荷時の状態に戻すことができます。

システムパスワードのリセット:この機能を実行すると、以下のユーザのパスワードがリセットされます。

- root ユーザ（シェルユーザ）
- loginuser（シェルユーザ）
- admin（事前に定義されている管理者アカウント）

さらに、システムを停止するには、「*後でシステムをシャットダウン*」オプションを選択します。

セキュリティに関する注記 – 次に WebAdmin に接続する人に対して、「*admin パスワード設定*」ダイアログウインドウが表示されます。したがって、パスワードをリセットしたら、すぐにログアウトし、ブラウザでそのページをリロード（再読み込み）して、新しい admin パスワードを設定してください。

また、「マネジメント > システム設定 > シェルアクセス」タブで新しいシェルパスワードを設定しない限り、シェルアクセスは実行できなくなります。

出荷時設定に初期化する:この機能は、工場出荷時のデフォルトの設定にデバイスをリセットします。以下のデータが削除されます。

- システム設定
- Web フィルタキャッシュ
- ログおよびレポーティングデータ
- データベース
- 更新パッケージ
- ライセンス
- パスワード
- 冗長化ステータス

ただし、Sophos UTMソフトウェアのバージョン番号はそのままです。つまり、インストールされたすべてのファームウェアおよびパターンの更新が維持されるということです。

注 –Sophos UTM は、出荷時設定への初期化が開始するとシャットダウンします。

4.2 WebAdmin 設定

「マネジメント > *WebAdmin 設定*」の下にあるタブで、TCP ポート、ユーザ設定、および WebAdmin の言語といった WebAdmin の基本設定を構成できます。

4.2.1 一般

「*WebAdmin 設定* > *一般*」タブで、WebAdmin 言語と基本アクセス設定を構成できます。

WebAdmin 言語

WebAdmin の言語を選択します。選択した言語は WebAdmin の出力にも一部使用されます。(例: メール通知やエグゼクティブレポートなど)これはグローバル設定で、すべてのユーザに適用されます。設定を保存するには「*適用*」をクリックします。

言語を変更した後は、すべてのテキストが正しい言語で表示されるようにブラウザのキャッシュを空にする必要がある場合があります。

WebAdmin アクセス設定

ここで、WebAdmin へのアクセスが許可されるユーザやネットワークを設定できます。

許可する管理者: Sophos UTMSophos UTM は同時に複数の管理者によって管理できます。「*許可された管理者*」ボックスで、WebAdmin インタフェースへの無制限の読み取りおよび書き込みアクセスを持つユーザまたはグループを指定できます。デフォルトでは、これは *SuperAdmins* のグループになります。

許可ネットワーク:「*許可ネットワーク*」ボックスで、WebAdmin インタフェースに接続できるネットワークを定義できます。UTMをスムーズにインストールするために、デフォルトは「すべて」になっています。これは、WebAdmin インタフェースはどこからでもアクセスできることを意味します。この設定は、できるだけ早く内部ネットワークに変更してください。ただし、最もセキュアなソリューションは、HTTPS 経由の 1台の管理者用 PC のみにアクセスを制限することです。

アクセストラフィックをログ:すべての WebAdmin アクセスアクティビティをファイアウォールログにログする場合は、「*アクセストラックをログ*」チェックボックスにチェックを入れます。

4.2.2 アクセス制御

「*WebAdmin 設定 > アクセス制御*」タブで、特定のユーザに対して WebAdmin ロールを作成することができます。これにより、WebAdmin ユーザに付与できる権限を細かく定義することができます。

以下の 2つのユーザロールがあらかじめ定義されています。

AUDITOR(監査担当者):このロールのユーザは、ログデータやレポートデータを参照できます。

READONLY(読取専用):このロールのユーザは、WebAdmin 内のすべてを参照できますが、編集、作成、削除は一切できません。

これらのいずれかのロールをユーザまたはグループに割り当てるには、「*編集*」ボタンをクリックし、各ユーザまたはグループを「メンバ」ボックスに追加します。

セキュリティポリシーに応じて、追加のロールを作成することができます。以下の手順に従ってください。

1. **「*アクセス制御*」タブで、「*新規ロール*」をクリックします。**
   「*ロールの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:この定義を説明する名前を入力します。

   メンバー:このロールを割り当てるユーザとグループをこのボックスに追加します。

読取専用アクセスのみ許可(オプション):このチェックボックスにチェックを入れると、WebAdmin のすべてのエリアへの読取専用アクセスが、指定メンバーに付与されます。

権限:このボックスでは、WebAdmin の異なる職種(Auditor:監査担当者とManager:管理者)に対し、異なる権限レベルが含まれています。Managerは各機能に対する完全な管理権限を持ちますが、Auditorは参照権限のみです。権限の前にあるチェックボックスにチェックを入れて、1つ以上の権限を選択することができます。
例:ユーザ Jon Doe に、メールプロテクションのManager権限を付与し、追加で「*読取専用アクセスを付与*」チェックボックスにチェックを入れるとします。このユーザは、メールプロテクションのセクションでは設定を変更できますが、WebAdmin のその他のエリアでは参照のみ可能で、変更は一切できません。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   設定が保存されます。

ロールを編集または削除するには、対応するボタンをクリックします。*AUDITOR*と*READONLY*の各ロールは削除できません。

4.2.3 HTTPS 証明書

「*マネジメント > WebAdmin 設定 > HTTPS 証明書*」タブで、WebAdmin CA 証明書をブラウザにインポートしたり、WebAdmin 証明書を再生成したり、WebAdmin とユーザポータルでの署名証明書の使用を選択したりできます。

WebAdmin アクセスの初回セットアップ時に、ローカル CA 証明書をUTMで作成しました。この CA 証明書の公開鍵をお使いのブラウザにインストールすると、WebAdmin インタフェースへのアクセス時にセキュリティ警告が表示されなくなります。

CA 証明書をインポートするには、以下の手順に従います。

1. **「*HTTPS 証明書*」タブで「*CA 証明書をインポート*」をクリックします。**
   CA 証明書の公開鍵がエクスポートされます。

   CA 証明書の公開鍵は、ディスクに保存するか、お使いのブラウザにインストールできます。

2. **証明書をインストールします**(オプション)。
   ブラウザにダイアログボックスが表示され、証明書のインストールをすぐに選択できます。

注 – システム時刻とタイムゾーンの違いによって証明書を作成してもすぐに有効にならない場合があります。この場合、ほとんどのブラウザでは、証明書が期限切れであると表示されますが、この表示は間違っています。ただし、証明書は 24時間以内には自動的に有効になり、その後 27 年間有効期間が持続します。

WebAdmin 証明書の再生成

WebAdmin 証明書は、お客様が初回ログイン時に指定したホスト名を参照します。その間にホスト名が変更された場合は、ブラウザがセキュリティ警告を表示します。この問題を避けるために、新しいホスト名を考慮に入れて証明書を作成できます。このようなホスト名を入力して「*適用*」をクリックします。証明書の変更後、WebAdmin で引き続き作業を行うには、多くの場合、お使いの Web ブラウザでページをリロード（再読み込み）し、新しい証明書を承認して、Webadmin に再度ログインする必要があります。

WebAdmin/ユーザポータル証明書の選択

CA 証明書をインポートする代わりに、独自に署名した証明書を WebAdmin およびユーザポータルで使用したい場合、ここでその証明書を選択します。ただし、ドロップダウンリストで証明書を選択できるようにするためには、最初に「*リモートアクセス > 証明書管理 > 証明書*」タブにおいて、証明書、CA、秘密鍵が含まれる証明書を PKCS#12 形式でアップロードする必要があります。アップロードされた証明書を使用するには、「*証明書*」ドロップダウンリストから選択し、「*適用*」をクリックします。

4.2.4 ユーザ設定

「*マネジメント > WebAdmin 設定 > ユーザ設定*」タブで、現在ログインしているユーザのためにグローバルショートカットやページあたりのアイテムといったユーザプリファレンス（基本設定）を構成できます。

WebAdmin ショートカットの設定

ここでは、多くの設定に使用されるドラッグ &ドロップのオブジェクトリストを開いたり閉じたりするためのキーボードショートカットを設定できます（詳細は、「*WebAdmin > オブジェクトリスト*」を参照）。また、検索ボックスのカーソルフォーカスを設定できます（「*WebAdmin > WebAdmin メニュー*」を参照）。ドロップダウンリストを使用して、Alt、Ctrl、Shift などの各種修飾キーとテキストボックスを選択し、異なる文字を入力してください。また、ドロップダウンリストで「*オフ*」を選択して、キーボードショートカットをオフにできます。

デフォルトの設定に戻るには、「*出荷時設定にリセット*」ボタンをクリックします。設定を保存するには「*適用*」をクリックします。

テーブルページャオプション

ここで WebAdmin のテーブルのページネーション（ページ割り）、つまり、ページあたりのアイテムの表示数をグローバルに定義できます。ドロップダウンリストをクリックして値を選択します。設定を保存するには「*適用*」をクリックします。

WebAdmin ブラウザタイトルのカスタマイズ

ここでは、WebAdmin ブラウザのウィンドウまたはタブに表示するラベルを変更できます。プレーンテキストを入力するか、次の変数を使用できます。

- %h: ホスト名
- %u: ユーザ名
- %i: リモート IP アドレス

デフォルト設定は、`WebAdmin - User %u - Device %h` で、これはたとえば、*WebAdmin – User admin – Device my_gateway.example.com* のように表示されます。設定を保存するには「*適用*」をクリックします。

4.2.5 詳細

WebAdmin アイドルタイムアウト

待ち時間:このフィールドでは、どれぐらい WebAdmin セッションのアイドル期間が続いたら管理者に再度ログインを要求するかを秒単位で指定できます。デフォルトでは、アイドルタイムアウトは 300秒に設定されています。指定できる範囲は 60～86,400秒です。

ダッシュボード画面でもログアウト: WebAdmin の「*ダッシュボード*」ページを開くと、自動ログアウト機能はデフォルトで無効になっています。ただし、このオプションを選択して、自動ログアウト機能をダッシュボードでも有効化することができます。

WebAdmin TCPポート

デフォルトでは、ポート `4444` を WebAdmin の TCP ポートとして使用します。「*TCP ポート*」ボックスには、`443` あるいは `1024`～`65535` の任意の値を入力できます。ただし、一部のポートは他のサービス用に予約されています。特に、ポート `10443` は使用できません。また、ユーザポータルあるいは SSL リモートアクセスに使用しているものと同じポートは使用できません。WebAdmin にアクセスするときは、ブラウザのアドレスバーでポート番号を IP アドレスに（コロンで区切って）追加する必要があります。たとえば、`https://192.168.0.1:4444` のように指定します。

利用規約

会社ポリシーで、WebAdmin へのアクセスを求めるユーザに利用規約への同意を求めることができます。ユーザが WebAdmin にログインするたびに利用規約に同意することを要求するには、「*ログイン後に「利用規約」を表示*」チェックボックスにチェックを入れます。これにより、ユーザがログインすると利用条件が表示されるようになります。利用条件に同意しないと、再びログアウトされます。

必要に応じて利用規約の文面を変更することができます。設定を保存するには「*適用*」をクリックします。

Sophos UTM Improvement Program

現在の設定に関する一般的な匿名情報や検知したウイルスに関する情報をSophos UTMに転送することで、Sophos UTMの改善にご協力ください。この種の情報からユーザを特定することはありません。また特定することもできません。ユーザ固有の情報、つまりユーザ名、オブジェクト名、コメント、その他の個人情報を収集することはありません。ただし、Web フィルタのアンチウイルススキャンが有効になっている場合は、ウイルスが発見された URL 情報は送信されます。

情報は、SSL により暗号化してSophosに送信されます。送信されたデータは集計形式で保存されます。Sophosのソフトウェアアーキテクトは、このデータを基に設計関連の決定を行い、将来のバージョンのSophos UTMの向上に役立てます。

「*匿名化した使用状況統計を送信*」オプションを有効にすると、UTMでは次の情報を収集します。

- 設定と使用状況に関するデータ:システムから Sophos のサーバに週に一度、次のデータが送信されます。
    - 次のようなハードウェアおよびライセンス情報（所有者を除く):

```
processor Intel(R) Core(TM)2 Duo CPU E8200 @ 2.66GHz
memory 512MiB System Memory
eth0 network 82545EM Gigabit Ethernet Controller
id: UTM
version:9.000000
type: virtual
license: standard
mode: standalone
active_ips:2
system_id:58174596-276f-39b8-854b-ffa1886e3c6c
```

システム IDは、再インストールの後などに、システム情報が誤って 2回収集されることがないように確認できる範囲のみでUTMを識別します。

- 次のような機能の使用状況（有効か無効かの特定のみ）:

  ```
  main->backup->status:1
  main->ha->status: off
  ```

- 次のような設定オブジェクトの数：

  ```
  objects->interface->ethernet:2
  objects->http->profile:5
  ```

- 過去 7日間の CPU、メモリおよびスワップの使用状況（%）

- ウイルスデータ:システムは次のデータをファイルに書き込み、15分おきに Sophos のサーバに自動アップロードします。
  - Web プロテクションにより検知されたウイルスに関する情報（例: 脅威名、MIME タイプ、要求した URL、ファイルサイズなど）
- IPS（侵入防御の統計）:新しい警告があるか、1分おきに IPS ログがチェックされます。新しい警告がある場合、ただちに次のデータが Sophos に送信されます。
  - Snort ルール ID やタイムスタンプなど、警告に関する情報。

4.3 ライセンス

Sophos UTMの特定の機能を使用できるか否かは、ライセンスとサブスクリプションによって定義されています。つまり、UTMとともに購入したライセンスとサブスクリプションに応じて、一部の機能は使用でき、他の機能は使用できなくなります。

4.3.1 ライセンスの取得方法

Sophos UTM には、すべての機能が有効になる 30日間のトライアルライセンスが付属しています。このライセンスの期限満了後にSophos UTMを操作したい場合には、有効なライセンスをインストールする必要があります。すべてのライセンス（無料のホームユーザライセンスを含む）はMyAstaroポータルで作成されます。

UTMライセンスの購入後に、アクティベーションキーがメールで送信されます。これらのキーを使用して、ライセンスを作成するか、既存のライセンスをアップグレードしてください。ライセンスを有効にするには、MyAstaro ポータルにログインし、ライセンス管理のページにアクセスしてください。

ページ上部にあるフォームの該当フィールドに、メールからアクティベーションキーをカット＆ペーストします。

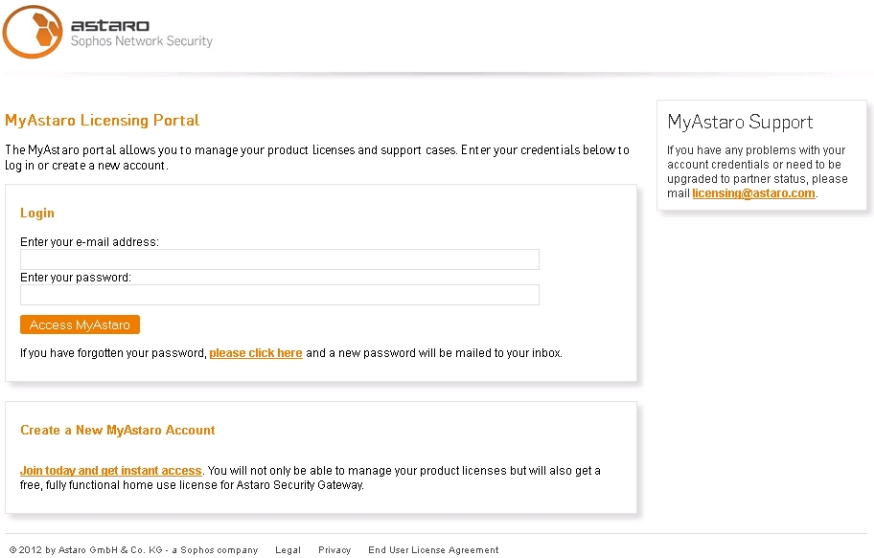

Figure 8 MyAstaro ポータル

別のフォームが表示されます。ここで、お客様がライセンスを購入した代理店についての情報と、お客様自身の詳細情報を入力してください。このフォームには、わかる限りの情報があらかじめ入力されています。また、該当する場合、SophosはUTMハードウェアのシリアル番号をこのフォームから収集します。フォームの送信後、ライセンスが作成され、ライセンス詳細ページが表示されます。ここで、ライセンスファイルをダウンロードすることができます。

ライセンスを実際に使用する場合、ライセンスファイルをハードドライブにダウンロードして、インストールされている WebAdmin にログインする必要があります。WebAdminで、「*マネジメント > ライセンス > インストレーション*」タブにアクセスし、アップロード機能を使用してハードドライブ上のライセンステキストファイルを検索します。ライセンスファイルをアップロードすると、WebAdmin がこれを処理して、すべてのサブスクリプションと、ライセンスに規定されたその他の設定を有効にします。

注 – メールで受信したアクティベーションキーを WebAdmin にインポートすることはできません。このキーは、ライセンスの有効化だけに使用されます。UTMにインポートできるのはライセンスファイルのみです。

4.3.2 ライセンスモデル

Sophosのモジュール式ライセンスモデルは非常に柔軟です。まず、基本ライセンスでは、基本機能を無料で提供しています(下の表を参照)。次に、6種類の追加サブスクリプションがあります。

- ネットワークプロテクション
- Web プロテクション
- Eメールプロテクション
- エンドポイントプロテクション
- ワイヤレスプロテクション
- Webサーバプロテクション

これらは、ニーズに合わせて個別に購入することも組み合わせて購入することもできます。FullGuard ライセンスにはすべてのサブスクリプションが含まれています。それぞれのサブスクリプションを使用して、製品の特定の機能を利用できます。下の表は、どのサブスクリプションでどの機能を使用できるかを示しています。

機能	基本ライセンス	ネットワーク	Web	Eメール	エンドポイント	ワイヤレス	Web サーバ
管理(バックアップ、通知、SNMP、SYM など)	✔						
ローカル認証(ユーザ、グループ)	✔						
基本ネットワーキング(スタティックルーティング、DHCP、DNS、Auto QoS、NTP など)	✔						
ファイアウォール/NAT (DNAT、SNAT など)	✔						
PPTP & L2TP リモートアクセス	✔						

機能	基本ライセンス	ネットワーク	Web	Eメール	エンドポイント	ワイヤレス	Web サーバ
ローカルログ、標準エグゼクティブレポート	✔						
侵入防御（パターン、DoS、フラッド、ポートスキャンなど）		✔					
IPsec & SSL サイト間 VPN、IPsec & SSL リモートアクセス		✔					
アドバンストネットワーキング（リンクアグリゲーション、リンクバランシング、ポリシールーティング、OSPF、マルチキャスト、カスタム QoS、サーバロードバランシング、ジェネリックプロキシなど）		✔	(✔)	(✔)			
ユーザポータル		✔	✔	✔			
冗長化（HA）		✔	✔	✔			
リモート認証（AD、eDir、RADIUS など）		✔	✔	✔			
リモートログ、詳細エグゼクティブレポート（アーカイブ、設定）		✔	✔	✔			
基本 Web フィルタリング & FTP プロキシ			✔				
Web & FTP マルウェアフィルタリング			✔				
アプリケーションコントロール			✔				

機能	基本ライセンス	ネットワーク	Web	Eメール	エンドポイント	ワイヤレス	Web サーバ
基本 SMTP プロキシ、隔離レポート、メールマネージャ				✔			
SMTP & POP3 マルウェアフィルタリング				✔			
エンドポイントプロテクション、アンチウイルス					✔		
エンドポイントプロテクション、デバイスコントロール					✔		
ワイヤレスプロテクション						✔	
Web サーバプロテクション							✔

また、UTM アプライアンス モデル 100 で選択可能なベーシックガードサブスクリプションもあります。これは、上記の基本機能を提供します（詳細は製品情報ページを参照してください）。

UTM機器は Sophos UTM Manager（SUM）経由で一括管理およびライセンス許可できます。この場合、SUM が MSP（Managed Service Provider）ライセンスをUTMに提供し、「*インストール*」タブは無効化されます。サブスクリプションは SUM サービスプロバイダーによってのみ有効化できます。

サブスクリプションとその機能セットについて詳しくは、認定UTMパートナーまたはSophos UTM Webページまでお問い合わせください。

サブスクリプションがないと、WebAdmin のタブが無効になります。タブの上には、ライセンス警告メッセージが表示されます。

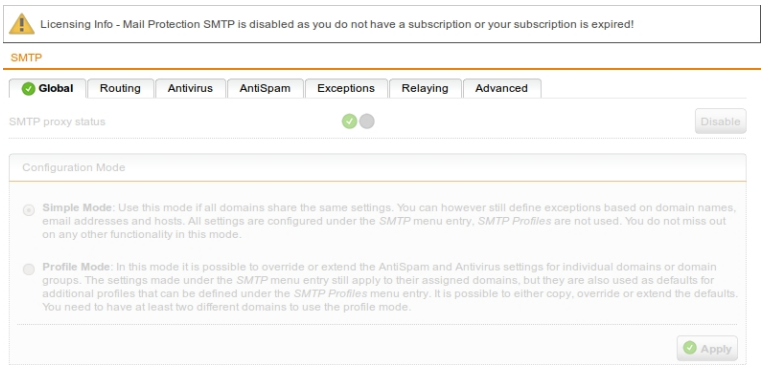

Figure 9 ライセンス:サブスクリプション警告メッセージ

Up2Date

各サブスクリプションは、自動アップデートを完全にサポートします。新しいファームウェアのアップデートがあると自動的に通知を受信します。また、ファームウェアとパターン更新を自動的にダウンロード(およびインストール)できます。

サブスクリプションなしの基本ライセンスでは、自動更新に制限があります。オンラインヘルプの更新などのパターン更新に限り、自動的にダウンロードされ、インストールされますが、使用可能なファームウェア更新については通知されず、ファームウェア更新は手動でダウンロードする必要があります。新しいファームウェアの通知はSophos UTM Up2Date ブログに表示されます。

サポートとメンテナンス

基本ライセンスには*Web サポート*が含まれます。Sophos UTM サポートフォーラムおよびSophos サポートデータベースを使用できます。

いずれかのサブスクリプションを購入すると、すぐに*標準サポート*に自動的にアップグレードされます。これにより、さらに MyAstaro ポータル でサポートを受けたり、認定済みのUTMパートナーに問い合わせをすることができます。

UTMエンジニアが担当者として 24時間年中無休のサポートを提供する*プレミアムサポート*サブスクリプションを購入することもできます。

4.3.3 概要

「*ライセンス > 概要*」タブには、ライセンスに関する詳細情報が表示され、次のように複数のエリアに分割されています。

- **基本ライセンス:**所有者、ID、登録日などの基本的なライセンスパラメータが表示されます。
- **ベーシックガード、ネットワークプロテクション、Eメールプロテクション、Web プロテクション、Webサーバプロテクション、ワイヤレスプロテクション、エンドポイントプロテクション:**サブスクリプションに関する情報(購入したものか否か、有効化されているか、有効期限、および提供する機能の簡単な説明など)が表示されます。

  注 –MSP ライセンスを使用している場合は、ライセンスは Sophos UTM Manager (SUM) で管理されているため、有効期限は表示されません。従来のキーおよびサブスクリプションは SUM MSP システムに置き換えられます。SUM の管理についての詳細は、「*集中管理 > Sophos UTM Manager*」を参照してください。

- **サポートサービス:**サポートレベルと有効期限が表示されます。

4.3.4 インストール

「*マネジメント > ライセンス > インストール*」タブでは、新しいライセンスのアップロードおよびインストールを実行できます。

注 –MSP ライセンスを使用している場合は、ライセンスは Sophos UTM Manager (SUM) で管理されているため、タブは無効化されています。新しいライセンスは SUM サービスプロバイダーによってインストール可能です。SUM の管理についての詳細は、「*集中管理*」>「*Sophos UTM Manager*」を参照してください。

ライセンスをインストールするには、次の手順に従ってください。

1. **「*ファイルのアップロード*」ダイアログボックスを開きます。**
   「*ライセンスファイル*」ボックスの横にあるフォルダアイコンをクリックします。

   「*ファイルのアップロード*」ダイアログボックスが開きます。

2. **ライセンスファイルを選択します。**
   ライセンスファイルが保存されているディレクトリを参照します。

   アップロードするライセンスファイルを選択します。

3. **「*アップロード開始*」をクリックします。**
   ライセンスファイルがアップロードされます。

4. **「*適用*」をクリックします。**
   ライセンスがインストールされます。新しいライセンスは、すでにインストールされている他のライセンスを自動的に置き換えます。

ライセンスのインストールには約 60秒かかります。

4.3.5 アクティブな IP アドレス

ユーザ（IP アドレス）が無制限に許可されるライセンスをお持ちでない場合は、お客様のライセンスでカバーされるIP アドレスに関する情報がこのタブに表示されます。お客様のライセンスの範囲外となるIP アドレスは、別のリストに記載されています。制限を超えると、定期的にメール通知が送信されます。

注 – 7日間にわたって使用されなかったIP アドレスは、ライセンスカウンタから自動的に削除されます。

4.4 Up2Date

「*マネジメント > Up2Date*」メニューを使用して、Sophos UTMの更新サービスを設定できます。定期的に更新パッケージをインストールすることで、UTMをバグフィックス、製品改善機能、ウイルスパターンなどが最新に保たれます。各更新パッケージは、によってSophosデジタル署名されています。署名がないものや偽造された更新は拒否されます。

2種類の更新を利用できます。

- **ファームウェアの更新:**ファームウェアの更新には、Sophos UTMソフトウェアのバグフィックスおよび拡張機能が含まれています。
- **パターンの更新:**パターンの更新によって、アンチウイルス、アンチスパム、IPSのルール、およびオンラインヘルプが最新状態に保たれます。

Up2Date パッケージをダウンロードするために、UTMは更新サーバに対する TCP 接続をポート `443` で開きます。このため、この接続は管理者の調整なしで使用できます。ただし、途中に別のファイアウォールがある場合は、ポート `443` TCP を介した更新サーバへの通信を明示的に許可する必要があります。

4.4.1 概要

「*マネジメント > Up2Date > 概要*」タブには、お使いのシステムが最新のものであるかどうかを示す概要が表示されます。ここで、新しいファームウェアやパターンの更新パッケージをインストールできます。

Up2Date 進行状況

このセクションはインストールプロセスを開始した場合のみ表示されます。「*Up2Date の進行状況を新しいウィンドウで確認する*」ボタンをクリックして、更新の進行状況をモニタしてください。ブラウザでポップアップウインドウの表示を禁止していない限り、更新の進行状況を示す新しいウインドウが表示されます。表示されない場合は、ポップアップウインドウを明示的に許可する必要があります。

注 – インストールプロセスが開始する前に、標準バックアップメール受信者にバックアップが送信されます。

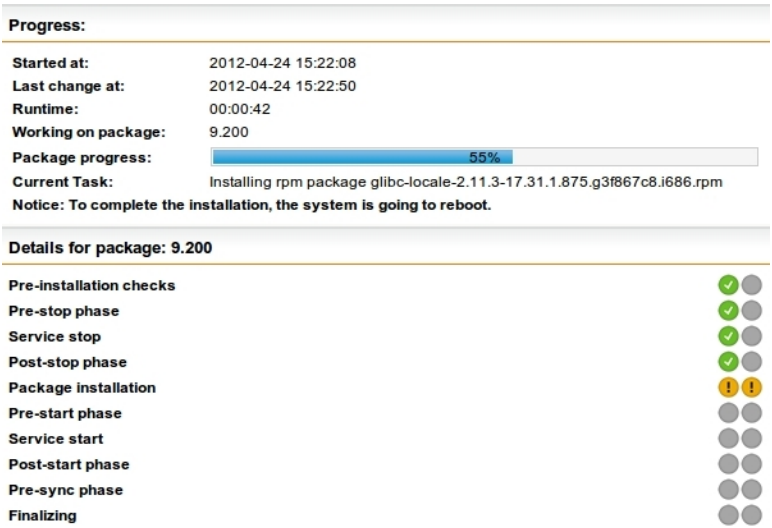

Figure 10 Up2Date:進捗ウィンドウ

ファームウェア

「ファームウェア」セクションには、現在インストールされているファームウェアのバージョンが表示されます。更新パッケージが利用できる場合は、「*すぐに最新バージョンに更新*」ボタンが表示されます。また、「*利用可能なファームウェアの概要*」セクションにメッセージが表示されます。ここで最新の更新パッケージを直接ダウンロードしてインストールできます。「*すぐに最新バージョンに更新*」をクリックすると、新しいウインドウに更新の進行状況が表示されます。これには、Webadmin の「*リロード*」ボタンをクリックします。

利用可能なファームウェアの概要

「*設定*」タブで「*手動*」を選択すると、このセクションに「*すぐに Up2Date パッケージを確認*」ボタンが表示されます。このボタンを使用して、ファームウェアの Up2Date パッケージを手動でダウンロードできます。Up2Date が複数利用できる場合は、どれをインストールするかを選択できます。最新のバージョンを直接インストールする場合は、「*ファームウェア*」セクションで「*すぐに最新バージョンに更新*」ボタンを使用できます。
各 Up2Date には「*スケジュール*」ボタンがあり、更新パッケージを自動的にインストールする日時を指定できます。スケジュールしたインストールを取り消す場合は、「*キャンセル*」をクリックします。

「暗黙的」インストールに関する注記:スケジュールした Up2Date パッケージが、古い Up2Date パッケージを最初にインストールすることを必要とする場合があります。その場合、この古い Up2Date パッケージは、実際の Up2Date パッケージの前にインストールするよう自動的にスケジュールされます。このパッケージに特定のタイミングを指定することもできますが、そのインストールを止めることはできません。

パターン

「*パターン*」セクションには、インストールしたパターンの現在のバージョンが表示されます。「*設定*」タブで「*手動*」を選択すると、「*すぐにパターンを更新*」ボタンが表示されます。このボタンを使用して、使用可能な新しいパターンをダウンロードしてインストールします。

注 –UTMを正常に動作させるために、現在のパターンバージョンと利用可能な最新のパターンバージョンが一致している必要はありません。お使いのユニットに新しいパターンを適用できない場合は、現在のパターンバージョンと利用できる最新パターンバージョンが異なってきます。どのパターンをダウンロードするかは、お客様の設定とハードウェアの構成によります。たとえば、Sophos UTMのIPS機能を使用しない場合は、新しく利用可能になった IPS パターンはインストールされません。このようにして、現在インストールされているパターンバージョンと利用できる最新のパターンバージョンの開きが大きくなっていきます。

4.4.2 設定

デフォルトでは、新しい更新パッケージは自動的にUTMにダウンロードされます。

ファームウェアのダウンロード間隔

このオプションは、デフォルトで 15分に設定されています。つまり、Sophos UTMは、15分毎に利用できるファームウェアの更新を確認します。Sophos UTMは、利用できるファームウェア更新パッケージを自動的にダウンロードします（インストールは行いません）。これが行われる実際の時間

は、選択された間隔の制限内でランダムに決定されます。最長で「*マンスリー*」の間隔を指定できます。または、ドロップダウンリストから「*手動*」を選択することで、ファームウェアの自動ダウンロードを無効にできます。「*手動*」を選択した場合は、「*すぐに Up2Date パッケージを確認*」ボタンが「*概要*」タブに表示されます。

パターンのダウンロード/インストール間隔

このオプションは、デフォルトで15分に設定されています。つまり、Sophos UTMは、15分毎に利用できるパターンの更新を確認します。Sophos UTMは、利用できるパターン更新パッケージを自動的にダウンロードしてインストールします。これが行われる実際の時間は、選択された間隔の制限内でランダムに決定されます。最長で「*マンスリー*」の間隔を指定できます。または、ドロップダウンリストから「*手動*」を選択することで、パターンの自動ダウンロードとインストールを無効にできます。「*手動*」を選択した場合は、「*すぐにパターンを更新*」ボタンが「*概要*」タブに表示されます。

4.4.3 詳細

「*マネジメント > Up2Date > 詳細*」タブで、詳細な Up2Date オプションを設定できます。たとえば、UTM用に親プロキシまたは Up2Date キャッシュを選択することなどができます。

注 – 更新パッケージはSophos UTM FTP サーバからダウンロードできます。

手動 Up2Date パッケージアップロード:UTMが新規更新パッケージを直接ダウンロードするためにインターネットまたは Up2Date キャッシュに直接アクセスできない場合は、更新パッケージを手動でアップロードできます。手動でアップロードするには、以下の手順に従います。

1. **「*ファイルのアップロード*」ダイアログボックスを開きます。**
   「*Up2Date ファイル*」ボックスの横にあるフォルダアイコンをクリックします。

   「*ファイルのアップロード*」ダイアログボックスが開きます。

2. **更新パッケージを選択します。**
   「*ファイルのアップロード*」ダイアログボックスの「*参照*」をクリックして、アップロードする更新パッケージを選択します。

3. **「*アップロード開始*」をクリックします。**
   更新パッケージがUTMにアップロードされます。

4. **「*適用*」をクリックします。**
   設定が保存されます。

親プロキシ

親プロキシは、多くの場合、政府承認のプロキシサーバを通してインターネットアクセスをルーティングする必要のある国などで必要とされます。親プロキシの使用がセキュリティポリシーで求められている場合、ここでホスト定義とポートを選択して親プロキシを設定できます。

親プロキシを使用:親プロキシの使用を有効にするには、チェックボックスにチェックを入れます。プロキシのホスト名とポートを入力します。

プロキシ認証が必要:親プロキシで認証が必要な場合、ここでユーザ名とパスワードを入力します。

親プロキシが設定されている場合は、Sophos UTMはファームウェアとパターンの Up2Date の両方を親プロキシからフェッチします。

4.5 バックアップ/リストア

バックアップ/リストア機能を使用すると、UTMの設定をローカルディスク上のファイルに保存することができます。このバックアップファイルを使用すると、新しいシステムや設定が誤っているシステムに、適切であるとわかっている設定をインストールすることができます。

システムに変更を加えるたびに忘れずにバックアップをとってください。これにより、常に最新の設定を使用できるようになります。さらに、バックアップは安全な場所に保存してください。この理由は、証明書や暗号化鍵といったセキュリティ関連のデータも含まれているためです。バックアップの生成後、読み取り可能であることを必ずチェックしてください。外部プログラムを使用してMD5チェックサムを生成すると良いでしょう。これにより、バックアップの完全性を後でチェックすることができます。

4.5.1 バックアップ/リストア

「*マネジメント > バックアップ/リストア > バックアップ/リストア*」タブでは、バックアップの作成やインポートに加え、既存のバックアップのリストア、ダウンロード、送信、削除ができます。

使用可能なバックアップ

このセクションは、自動バックアップ機能か手動により以前に1つ以上のバックアップが作成されている場合にのみ表示されます(「*バックアップの作成*」のセクションを参照してください)。

すべてのバックアップが、作成日時、UTMバージョン番号、作成ユーザ、コメントと共にリストされます。

バックアップに対して、ダウンロード、リストア、削除、送信を実行できます。

- **ダウンロード:**開いたダイアログウィンドウで、暗号化されたファイル(パスワードを指定)または暗号化されていないファイルのダウンロードを選択できます。「*バックアップのダウンロード*」をクリックします。ダウンロードするバックアップを保存するファイルシステム内の場所を選択するよう求められます。
    - **ダウンロード前に暗号化:**バックアップのダウンロードまたは送信の前に、バックアップを暗号化することもできます。CBC モードでの暗号化は、Blowfish 暗号によって行われます。パスワードを入力します(確認のために 2回入力します)。バックアップのインポート時に、このパスワードが求められます。暗号化されたバックアップのファイル拡張子は `ebf`、暗号化されていないバックアップのファイル拡張子は `abf` です。

      注 – バックアップには、管理者パスワード、HA パスフレーズ(設定している場合)、すべての RSA 鍵および X.509 証明書が含まれます。これは機密情報なので、暗号化を有効にするのが賢明です。

- **リストア:**現在のシステム設定をバックアップに保存されている設定に変更します。リストア後に再度ログインする必要があります。選択したバックアップにすべてのデータが含まれている場合、すぐにログインできます。選択したバックアップにすべてのデータが含まれていない場合(「*バックアップの作成*」のセクションを参照)、ログイン過程で必要なデータを入力する必要があります。選択したバックアップでホストデータのみが削除されている場合は、必要に応じて管理者のメールアドレスを追加することができます。この情報は受信者が指定されていない場合に使用されるか、複数受信者を指定できる場合に追加アドレスとして使用されます。
    - USB フラッシュドライブからのバックアップのリストア:USB スティックなどの FAT フォーマットされた USB フラッシュドライブから、暗号化されていないバックアップファイル(ファイル拡張子 `abf`)をリストアすることもできます。USB フラッシュドライブからバックアップをリストアするには、バックアップファイルを USB フラッシュドライブにコピーして、ブート(起動)前にデバイスをSophos UTMにプラグインします。デバイスに複数のバックアップファイルが保存されている場合、辞書的に最初のファイルが使用されます(数字は文字より優先します)。たとえば、バックアップファイルである `gateway_backup_2012-04-17.abf` および `2011-03-20_gateway_backup.abf` の両ファイルが USB フラッシュドライブに保存されているとします。ブート時に使用されるのは 2つ目のファイルです。このファイルはもう一方より日時が古いのですが、ファイル名の先頭が数字であるためです。

さらに、バックアップのリカバリが成功するとロックファイルが作成され、USB フラッシュドライブが接続されている間に同じバックアップが何度も繰り返しインストールされることを防ぎます。前のバックアップを再びインストールしたい場合には、USB フラッシュドライブを接続していない状態で再起動する必要があります。これにより、すべてのロックファイルが削除されます。再び USB フラッシュドライブを接続してからブートすると、同じバックアップをインストールすることができます。

- **削除:**リストからバックアップを削除します。リストの下部の削除アイコンを使用して、選択したバックアップをすべて削除できます。バックアップを選択するには、バックアップの左横のチェックボックスをクリックするか、リスト下部のチェックボックスを使用してすべてのバックアップを選択するかします。
- **送信:**開いたダイアログウィンドウで、暗号化されたファイル(パスワードを指定)または暗号化されていないファイルの送信を選択できます。「*直ちに送信*」をクリックしてバックアップを送信します。受信者は標準受信者となります。つまり、「*自動バックアップ*」タブに指定したアドレスに、バックアップが送信されます。
    - **送信前に暗号化:**上記の*ダウンロード前に暗号化*を参照してください。

バックアップの作成

バックアップは、(予期しない)変更または故障の後でシステムをリストアするために便利なだけではありません。類似の設定にするシステムをセットアップする際のテンプレートとして使用し、これらのシステムをあらかじめある程度設定しておくことで、時間を大幅に節約できます。そのためには、バックアップを作成する前に、ホスト名、証明書など特定の情報を削除しておくことができます。

現在のシステム状態のバックアップを作成するには、次の手順に従います。

1. **「*バックアップの作成*」セクションに、コメントを入力します**(オプション)。
   コメントは、バックアップリストでバックアップとともに表示されます。
2. **次の設定を行います**(オプション)。

   一意のサイトデータ(Unique site data)の削除:ホスト固有のデータなしでバックアップを作成するには、このオプションを選択します。この対象となるのは、ホスト名、システム ID、SNMP データ、HA データ、ライセンス、シェルユーザパスワード、匿名パスワード、ならびにメールプロテクション、Webプロテクション、クライアント認証、IPsec、SSL VPN、RED、WebAdmin、Webアプリケーションファイアウォール、およびプロキシ用のすべての証明書、公開鍵と秘密鍵、および指紋とシークレットなどです。
   このようなバックアップは、類似のシステムを複数セットアップするために便利です。ただし、いくつか考慮すべき点があります。1)リストア後は、基本システムセットアップになります。2)最初のインタフェースのみが設定されています。プライマリ IP アドレスは、インストール中に

構成される設定の 1つです。他のすべてのインタフェースは無効になり、IP アドレスが 0.0.0.0 に設定されます。

警告 – ほとんどのホスト固有データが削除されても、このようなバックアップテンプレートにはユーザパスワードなどの機密情報がまだ含まれています。そのため、暗号化することをお勧めします。

管理者メールアドレスの削除:UTMの様々な部分（メールプロテクションのポストマスタアドレス、通知など）で使用される管理者のメールアドレスを追加で削除するには、このオプションを選択します。このオプションは、顧客のサイトでSophos UTMデバイスをセットアップするIT パートナーにとって特に便利です。

3. **「*バックアップを直ちに作成*」をクリックします。**
   使用可能なバックアップのリストに、バックアップが表示されます。

   これらのオプションのいずれかまたは両方を選択してバックアップを作成した場合には、バックアップエントリにそれぞれの追加コメントが含まれるようになります。

バックアップのインポート

バックアップをインポートするには、フォルダアイコンをクリックし、アップロードするバックアップファイルを選択してから、「*アップロード開始*」をクリックしてください。暗号化されたバックアップファイルをインポートする場合、バックアップのインポート前に、正しいパスフレーズを入力する必要があります。バックアップはすぐにリストアされるのではなく、「*使用可能なバックアップ*」リストに追加されます。

4.5.2 自動バックアップ

「*マネジメント > バックアップ/リストア > 自動バックアップ*」タブでは、バックアップの自動生成に関する複数のオプションを設定することができます。バックアップを自動的に作成するためには、次の手順に従います。

1. **「*自動バックアップ*」タブで自動バックアップを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、「*オプション*」および「*バックアップをメール送信*」エリアが編集可能になります。

2. **間隔を選択します。**
   自動バックアップは、さまざまな間隔で作成することができます。

デイリー、ウィークリー、マンスリーから選択できます。

3. **保存する最大バックアップ数を指定します。**
   ここで指定した数まで、バックアップが保存されます。最大値に到達すると、一番古いバックアップが削除されます。

   この対象となるのは、自動作成されたバックアップのみです。システム更新の前に手動で作成されたバックアップや 自動的に作成されたバックアップは削除されません。

4. **「*適用*」をクリックします。**
   設定が保存されます。

UTMのバックアップ作業を簡素化するために、バックアップ機能では、定義したメールアドレスのリストに対して、バックアップファイルをメールで送信することができます。

受信者:自動的に生成されたバックアップは、「*受信者*」ボックスに含まれるユーザに送信されます。複数のアドレスを追加できます。デフォルトでは、最初の管理者のメールアドレスが使用されます。

メールバックアップの暗号化:さらに、オプションでバックアップを暗号化できます(3DES 暗号化)。

パスワード:「*暗号化*」のオプションを選択したら、パスワードを入力します(確認のために 2回)。バックアップのインポート時に、このパスワードが求められます。

自動的に作成されたバックアップは、「*作成者*」を示す `System` フラグ付きで「*バックアップ/リストア*」タブの「*使用可能なバックアップ*」リストに表示されます。ここで、自分で作成したバックアップと同様に、リストア、ダウンロード、削除を実行できます。

4.6 ユーザポータル

Sophos UTMのユーザポータルは、許可したユーザにパーソナルなメールおよびリモートアクセスサービスを提供する特別なブラウザベースアプリケーションです。ユーザポータルにアクセスするには、Sophos UTMの URL(`https://192.168.2.100` など)にブラウズします(HTTPS プロトコルを使用していることと、WebAdmin インタフェースにアクセスするために通常入力するポート番号 `4444` がないことに注意)。

ユーザポータルは、メール隔離を始めとする機能を備えています。メール隔離は、悪意あるソフトウェアに感染したメッセージ、不審な添付物を含むメッセージ、スパムと特定されたメッセージ、または明確に禁止した表現を含むメッセージを保持します。

ログインページで、ユーザはヘッダバーの右側にあるドロップダウンリストから言語を選択できます。

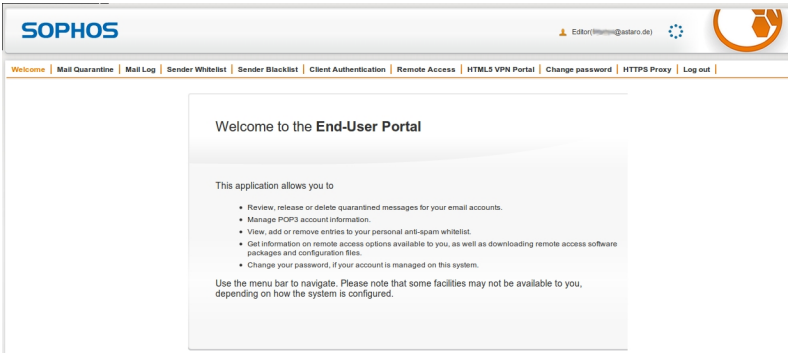

Figure 11 ユーザポータル:Welcome ページ

ユーザポータルで、ユーザは以下のサービスにアクセスできます。

- **SMTP 隔離:**ユーザは隔離場所に保持されているメッセージを表示したり、リリースできます。どのタイプのメッセージをユーザがリリースできるかは「*Eメールプロテクション > 隔離レポート > 詳細*」タブで決定できます。(このタブは、POP3 が無効な場合は「*メール隔離*」となります。)
- **SMTP ログ:**ここでは、ユーザはメールトラフィックの SMTP ログを表示できます。(このタブは、POP3 が無効な場合は「*メールログ*」となります。)
- **POP3 隔離:**ユーザは隔離場所に保持されているメッセージを表示したりリリースできます。どのタイプのメッセージをユーザがリリースできるかは「*Eメールプロテクション > 隔離レポート > 詳細*」タブで決定できます。(このタブは、SMTP が無効な場合は「*メール隔離*」となります。)
- **POP3 アカウント:**ユーザは使用する POP3 アカウントの資格情報を入力できます。POP3 アカウント情報が入力されたスパムメールのみがユーザポータルに表示されます。POP3 アカウントのアカウント情報が保存されているユーザは、各メールアドレスについて、別々の隔離レポートを受け取ります。許可される POP3サーバは「*Eメールプロテクション > POP3 > 詳細*」タブで指定する必要があります。
- **送信者ホワイトリスト:**ここで送信者をホワイトリストに追加することで、それらの送信者から送信されたメッセージがスパムとして分類されないようにできます。ただし、ウイルスを含むメールやスキャン不可能なメールは隔離されます。ホワイトリスト内の送信者は、有効なメールアドレス (例: `jdoe@example.com`) またはアスタリスクをワイルドカードとして使用して特定ドメインの全メールアドレス (例: `*@example.com`) を指定できます。
- **送信者ブラックリスト:**ここでユーザはメール送信者 (例: `phishing@hotmail.com`) をブラックリストに追加するか、ドメイン全体 (例: `*@hotmail.com`) をブラックリストに追加するこ

とができます。ブラックリストは、システム内で SMTP とPOP3 が使用されていれば、SMTP とPOP3 の両方のメールに適用されます。ブラックリストに送信者を追加するには、「+」アイコンをクリックしてアドレスを入力し、チェックアイコンをクリックして保存します。

- **ホットスポット:**ここでユーザは、ホットスポットのアクセスデータを確認して管理できます。このタブは、特定のユーザに対して 1つ以上のホットスポットが有効にされている場合にのみ使用できます。当日有効パスワードタイプのホットスポットには、現在のパスワードの表示と変更を行うことができます。バウチャータイプのホットスポットには、バウチャーの生成、印刷、エクスポート、削除を行うことができます。生成バウチャーのリストには、使用状況の情報が表示されます。詳細は、「*ワイヤレスプロテクション > ホットスポット*」を参照してください。

- **クライアント認証:**ここでユーザは、Sophos Authentication Agent（SAA）のセットアップファイルをダウンロードできます。SAA は Web フィルタの認証モードとして使用できます。「*クライアント認証*」タブは、クライアント認証が有効化されている場合にのみ使用できます。詳細は、「*定義とユーザ > クライアント認証*」を参照してください。

- **リモートアクセス:**ユーザはリモートアクセスクライアントソフトウェアおよびそれらに付属する設定ファイルをダウンロードできます。ただし、「*リモートアクセス*」タブは、その特定ユーザに対して最低 1つのリモートアクセスモードが有効になっている場合のみ利用できます。

- **HTML5 VPN ポータル:**ここでユーザは、定義済みのサービスを使用して定義済みのホストへの VPN 接続を確立することができます。このタブは、特定のユーザに対して 1つ以上の VPN 接続が有効にされている場合にのみ使用できます。詳細は、「*リモートアクセス > HTML5 VPN ポータル*」を参照してください。

- **パスワードの変更:**ユーザはユーザポータルにアクセルするためのパスワードを変更できます。

- **HTTPS プロキシ:**ユーザは HTTP/S プロキシ CA 証明書をインポートし、セキュア Web サイトへの訪問時に表示されるエラーメッセージを回避することができます。「*プロキシ CA 証明書をインポート*」をクリックすると、ユーザのブラウザに、他の目的に対して CA を信頼するか確認するプロンプトが表示されます。詳しくは、「*Web プロテクション > Web フィルタ > HTTPS CA*」の章を参照してください。

- **ログアウト:**ユーザポータルからログアウトするには、ここをクリックします。これは、ログイン時に「*ログインを記憶*」を選択した場合に（これによりクッキーが作成されます）、明示的にログアウトしてこのクッキーを削除したいときのみ必要です。そうでない場合は、この*ログアウト*のリンクを使用する必要はありません。ブラウザのタブまたはウインドウを閉じるだけで十分です。

4.6.1 グローバル

「*マネジメント > ユーザポータル > グローバル*」タブで、ユーザポータルを有効化できます。さらに、ユーザポータルへのアクセスを許可するネットワークとユーザを指定できます。

ユーザポータルへのアクセスを有効にするには、以下の手順に従います。

1. **ユーザポータルを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*エンドユーザポータルオプション*」エリアが編集可能になります。

2. **許可するネットワークを選択します。**
   ユーザポータルへのアクセスを許可するネットワークを選択します。

3. **許可するユーザを選択します。**
   ユーザポータルへのアクセスを許可するユーザまたはユーザグループを選択します。

   すべてのユーザにアクセスを許可しない場合は、「*全てのユーザを許可*」チェックボックスの選択を外し、ユーザとユーザグループを個別に選択します。

4. **「*適用*」をクリックします。**
   設定が保存されます。

4.6.2 詳細

「*詳細*」タブで、ユーザポータルの代替ホスト名とポート番号に加え、言語とセキュリティオプションを設定できます。

言語

ログイン時に、ユーザポータルは Web ブラウザの言語設定を取得し、それぞれのロケールをロードして、ブラウザのデフォルトと同じ言語でポータルを表示します。ブラウザの言語設定がユーザポータルで利用できない場合は、フォールバック（予備）の言語をここで選択できます。ユーザは、追加オプションとして、ユーザポータルのログインページで言語を選択できます。

セキュリティ

ユーザポータルは Cookie を使用してセッションを追跡します。永続的（固定）Cookieにより、セッションを閉じた後で再度ログインしないで戻ることが可能になります。これらはいつでもユーザ側で削除できますが、ユーザポータルの「*ログアウト*」ボタンを使用することが必要です。

ポータルメニューの無効化

ここにリストされているそれぞれの機能を WebAdmin で有効にすると、ユーザポータルにメニュー項目が表示されます。ただし、ここでは、ユーザポータルで表示しないメニュー項目を定義できます。これを定義するには、それぞれのオプションを選択して「*適用*」をクリックします。

ネットワーク設定

ホスト名:デフォルトで、これは「*マネジメント > システム設定 > ホスト名*」タブの UTM のホスト名です。ただし、インターネットを介してアクセスするユーザにユーザポータルへのアクセスを付与する場合は、パブリックに解決できる代替ホスト名をここに入力する必要があります。

Listen アドレス:デフォルトは「すべて」です。Web アプリケーションファイアウォールを使用する場合、サービスがユーザポータル接続をリスンするためのインタフェースアドレスを指定する必要があります。ユーザポータル接続ハンドラと Web アプリケーションファイアウォールが受信 SSL 接続を識別できるようにするために、この設定が必要です。

ポート:デフォルトでは、HTTPS のポート `443` が選択されています。ポートは、`1024`～`65535` の範囲内でどの値にでも変更できます。`10443` または *WebAdmin TCP ポート* は選択できません。これは「*マネジメント*」>「*WebAdmin 設定*」>「*詳細*」タブで設定されています。ユーザポータルは、定義したポートから独立しており、HTTPS のみを介して常にアクセスすることができます。

ウェルカムメッセージ

ユーザポータルのウェルカムメッセージをカスタマイズできます。シンプルな HTML マークアップとハイパーリンクを使用できます。

注 – ホームユーザライセンスを使用している場合は、ウェルカムメッセージを変更できません。

4.7 通知

Sophos UTM には、UTM で発生するあらゆる種類のセキュリティ関連イベントについて、メールまたは SNMP トラップで即時通知する機能が搭載されています。管理者が知るべきすべてのイベントが、各種エラー、警告、情報コードによって示されます。どのような通知が送信されるのかは、「*通知*」タブで設定した選択内容に応じて決まります。

4.7.1 グローバル

「*マネジメント > 通知 > グローバル*」タブでは、UTMが送信する通知メールに利用される送信者アドレス(*送信元*アドレス)を設定できます。デフォルトでは `do-not-reply@fw-notify.net` となっています。このアドレスを変更する場合、お客様のドメインのメールアドレスを入力することをお勧めします。この理由は、一部のメールサーバでは、指定された送信者アドレスが本当に存在することを確認するように設定されているためです。

さらに、UTM通知の受信者を指定することができます。デフォルトでは、初期セットアップ時に入力された管理者のメールアドレスです。

通知を制限:一部のセキュリティ関連イベント(検出された侵入試行など)では、大量の通知が発生し、通知受信者の受信トレイが短時間でいっぱいになる可能性があります。このため、Sophos UTMには、1時間あたりに送信される通知数を制限するための妥当なデフォルト値が用意されています。このオプションを無効にすると、「*マネジメント > 通知 > 通知*」タブで通知を送信するように設定されているすべてのセキュリティ関連のイベントから通知が発生します。

機器固有のテキスト

ここでは、Sophos UTMの説明(場所など)を入力できます。この情報は、送信される通知に示されます。

4.7.2 通知

通知は次の3つのカテゴリに分類されます。

- **CRIT:**UTM が操作不能になる可能性がある重大なイベントを通知するメッセージ。
- **WARN:**しきい値の超過など、ユーザの注意を必要とする潜在的な問題についての警告。
- **INFO:**システムコンポーネントの再起動など、情報提供目的のみのメッセージ。

通知をメールとSNMP トラップのいずれで送信するかを選択できます。

4.7.3 詳細

UTMでメールを直接送信できない場合、メールを送信するスマートホストを設定することができます。次の手順で実行します。

1. **「*マネジメント > 通知 > 詳細*」タブで「*外部 SMTP*」を有効にします。**
   トグルスイッチをクリックします。

2. **スマートホストを入力します。**
   ドラッグ &ドロップを使用できます。ポートは、デフォルトの SMTP ポートである 25 に事前設定されています。

   - **TLS を使用:**通知の送信で TLS を強制するには、このチェックボックスにチェックを入れます。スマートホストで TLS がサポートされない場合、通知は送信されません。

3. **認証設定を指定:**
   スマートホストが認証を要求する場合は、「*認証*」チェックボックスにチェックを入れて、該当するユーザ名とパスワードを入力します。

4. **「*適用*」をクリックします。**
   設定が保存されます。

4.8 カスタマイズ

「*マネジメント*」>*カスタマイズ*」のタブを使用すると、Sophos UTMが生成するメール通知とステータスメッセージをカスタマイズおよびローカライズして、会社のポリシーやコーポレートアイデンティティに合わせてこれらのメッセージを調整することができます。

さらに、カスタム Web テンプレートを編集およびアップロードして、ユーザがブロックメッセージやその他の通知を受信する方法をさらに変更することができます。

注 – ホームユーザライセンスを使用している場合は、カスタマイズできません。

4.8.1 グローバル

「*マネジメント*>*カスタマイズ*>*グローバル*」タブでは、ユーザに表示されるシステムメッセージのグローバル表示オプションをカスタマイズすることができます。UTF-8/Unicode がサポートされています。

ここでは、カスタマイズ可能なグローバルオプション(*会社ロゴ*および*カスタム会社テキスト*)や「*マネジメント*」>「*カスタマイズ*」>「*Web メッセージ*」ページで設定する「コンテンツのブロック」メッセージの例を示しています。

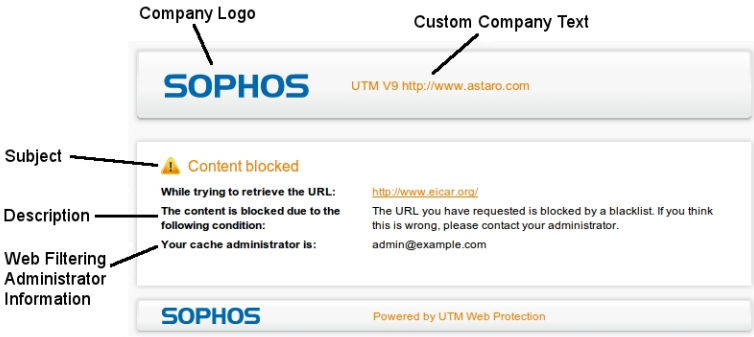

Figure 12 カスタマイズ:ブロックされるページの例とカスタマイズ可能な部分

カンパニーロゴ

カンパニーロゴ/バナーをアップロードし(png 形式のみ)、次の状況で使用することができます。

- Web メッセージ:
- 「ブロックされたPOP3 メール」用メッセージ
- (スパムメールが隔離場所からリリースまたはホワイトリスト化された後で隔離レポートに表示される)隔離リリースステータスメッセージ
- 隔離レポート

ユーザに表示される一部のメッセージはデフォルトのロゴに合わせて最適化されます(195 x 73 ピクセル、透明の背景)。見栄えを良くするには、同じ属性の画像を使用します。

ロゴのアップロード:

1. **「*ファイルのアップロード*」ダイアログボックスを開きます。**
   「*新しいロゴのアップロード*」ボックスの横にあるフォルダアイコンをクリックします。

   「*ファイルのアップロード*」ダイアログボックスが開きます。

2. **ロゴを選択します。**
   アップロードするロゴがある場所までブラウズします。

   ロゴを選択し、「*アップロード開始*」をクリックします。

3. **「*適用*」をクリックします。**
   ロゴがアップロードされ、すでにインストールされているファイルと置き換えられます。

カスタムカンパニーテキスト

Sophos UTMのウイルススキャナまたはコンテンツフィルタによってWeb サイトがブロックされたときに、カンパニーロゴの下に表示されるメッセージをカスタマイズします。ここには、管理者の連絡先データなどを入力することができます。

4.8.2 Web メッセージ

Sophos UTMによって表示されるWeb フィルタメッセージのテキストをカスタマイズします。メッセージの中には、大きすぎるファイル、特定の種類のファイル、またウイルスを含むファイルをユーザがダウンロードしようとして禁止される際に表示されるものがあります。また、その他のメッセージは、ユーザがファイルをダウンロードするときやUTMの認証を要求された場合に、禁止されたWeb サイトやアプリケーションにアクセスしようとして表示されるものもあります。これらのメッセージを他の言語に翻訳したり、顧客サポートの連絡先情報が表示されるように変更したりできます。

注 – 「*Web メッセージ*」タブのフィールドに入力したテキストはカスタムWeb テンプレートで参照できます。詳細は、「Web テンプレート」を参照してください。

以下のメッセージが設定可能です。

コンテンツのブロック

- **サーフプロテクション:**URL がブロック設定されているカテゴリーに一致するか、またはサイトレピュテーションが一定のしきい値以下であるWeb ページに、ユーザがアクセスしようとする際に、このメッセージは表示されます。詳細は、「*Webプロテクション*>*Web フィルタリング*」の章を参照してください。
- **ブラックリスト:**このメッセージは、ブラックリスト化されたURL と一致するWeb ページをユーザが取得しようとすると表示されます。URL をブラックリスト化する方法は、「*Web プロテクション*>*Webフィルタリング*>*URL フィルタリング*」を参照してください。
- **MIME タイプ:**このメッセージは、ブロックされたMIME タイプのファイルをユーザが要求すると表示されます。MIME タイプの詳細は、「*Web Protection*>*Web フィルタリング*>*ウイルス/マルウェア対策*」の章を参照してください。
- **ファイル拡張子:**このメッセージは、ブロックされたファイル拡張子をユーザが要求すると表示されます。ファイル拡張子の詳細は、「*Webプロテクション*>*Web フィルタリング*>*ウイルス/マルウェア対策*」の章を参照してください。

- **ファイルサイズ:**このメッセージは、ファイルサイズの上限を超えたファイルをユーザが要求すると表示されます。ダウンロードのサイズ制限を設定する方法は、「*Webプロテクション > Webフィルタリング > 詳細*」を参照してください。
- **アプリケーションコントロール:**このメッセージは、アプリケーションコントロールでブロックするように設定されている種類のネットワークトラフィックをユーザが使用しようとした場合に表示されます。アプリケーションコントロールに関する詳細は、「*Webプロテクション > アプリケーションコントロール*」を参照してください。
- **ウイルス検知:**このメッセージは、ウイルス感染が原因でファイルがブロックされた場合に表示されます。ウイルス保護の設定に関する詳細は、「*Webプロテクション > Web フィルタリング > ウイルス/マルウェア対策*」の章を参照してください。

ダウンロード/検索

- **ダウンロード中:**このステータスは、ファイルのダウンロード中に表示されます。「*ダウンロードマネージャ*」を参照してください。
- **ウイルススキャン実行中:**このメッセージはUTMが悪意のあるコンテンツを検索中に表示されます。「*ダウンロードマネージャ*」を参照してください。
- **ダウンロード官僚:**このメッセージは、ファイルのダウンロードと検索が完了し、安全が確認された後で表示されます。「*ダウンロードマネージャ*」を参照してください。

認証

- **透過モードの認証:**このオプションは、Web フィルタリングを透過モードで使用し、「ブラウザ」認証モードを選択している場合のみ適用されます。詳細は、「*Webプロテクション > Webフィルタプロファイル > プロキシプロファイル*」を参照してください。テキストは認証ページに表示されます。各ユーザは Web フィルタを使用する前にこの認証ページにログインする必要があります。「*利用条件*」フィールドに入力すると、認証ページに免責事項が表示されます。このフィールドが（デフォルトの設定のまま）空欄になっていると、免責事項は表示されません。
- **コンテンツブロックのバイパス:**このメッセージは、ページが サーフプロテクション によってブロックされ、ブロックバイパスオプションが有効になっている場合に表示されます（*「Web プロテクション」>「Web フィルタリング」>「URL フィルタリング」*を参照）。「*利用条件*」フィールドに入力すると、認証ページに免責事項が表示されます。このフィールドが（デフォルトの設定のまま）空欄になっていると、免責事項は表示されません。

エラー

- **サーバエラー:**このメッセージは、ユーザの要求を処理中にエラーが発生したときに表示されます。

管理者情報:ここでは、Web フィルタを管理する管理者に関する情報（管理者のメールアドレスなど）を入力できます。

4.8.2.1 Web メッセージの修正

コンテンツのブロック、ダウンロード/検索、認証、またはエラーなど各種メッセージを修正する手順は以下のとおりです。

1. **メッセージを選択します。**
   「ページ」ドロップダウンリストで、編集するエンドユーザメッセージを選択します。

   そのメッセージの「*件名*」および「*説明*」が表示されます。

2. **件名および説明を修正します。**
   必要に応じてデフォルトのテキストを編集します。

3. **「*適用*」をクリックします。**
   変更したテキストは保存されます。

4.8.2.2 ダウンロードマネージャ

Web フィルタが有効である場合、サイズが 1MB を超え、コンテンツタイプがテキストまたは画像以外であるコンテンツのダウンロード中、Web ブラウザに次のダウンロードページが表示されます。要求されているのが動画または音声ストリームである場合や、5秒以内にファイルの 50% 超のダウンロードが完了している場合には、ダウンロードページは表示されません。

ダウンロードページに表示される情報は「*Web メッセージ*」タブでカスタマイズできます。

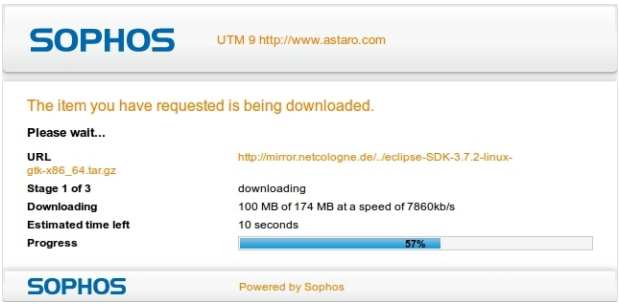

Figure 13 カスタマイズ:HTTP ダウンロードページ、ステップ 1/3ファイルダウンロード中

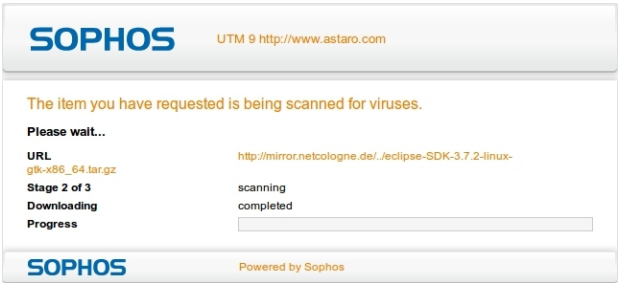

Figure 14 カスタマイズ:HTTP ダウンロードページ、ステップ 2/3ウイルススキャン中

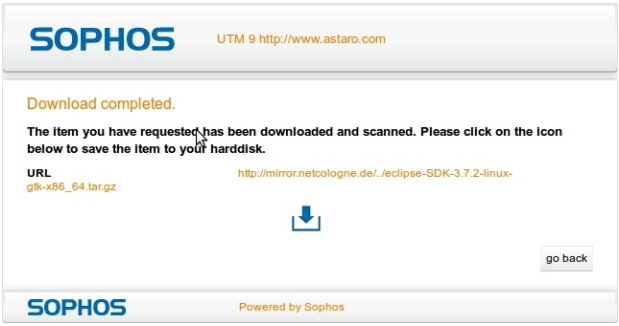

Figure 15 カスタマイズ:HTTP ダウンロードページ、ステップ 3/3ファイルのダウンロード完了

4.8.3 Web テンプレート

ユーザに表示されるメッセージの外観および内容をカスタマイズするには、HTML ファイルをSophos UTMにアップロードすることができます。例として、Sophosではいくつかのサンプルのテンプレートが準備されています。これらのテンプレートでは、各ユーザメッセージの情報を動的に挿入できる変数の使い方が示されています。たとえば、あるファイルがウイルスを含んでいるためにブロックされた場合、ブロックされたウイルスの名前を挿入する変数を含めることができます。

4.8.3.1 Web テンプレートのカスタマイズ

警告 –Sophos UTM通知のカスタマイズは上級者向けのトピックです。ここでのタスクは、HTML や JavaScript の知識が十分ある場合のみ実施してください。

ブロックメッセージ、ステータスメッセージ、エラーメッセージ、また認証要求など、カスタムバージョンのSophos UTM通知をアップロードすることができます。4つのサンプルテンプレートには、変数の

実例やサンプル画像が含まれます。カスタムのメッセージや通知文のひな型としてサンプルテンプレートを使用することも、独自の HTML ファイルをアップロードすることもできます。有効な変数については、Sophos サポートデータベースのUTM Web テンプレートで変数を使用するを参照してください。

「*Web メッセージ*」タブで設定したメッセージのテキストを使用する場合は、カスタムテンプレートで適切な変数を挿入できます。詳細は、「*Web メッセージ*」を参照してください。

サンプルのテンプレートおよび画像をダウンロードするには、以下のリンクをクリックして .zip ファイルを保存してください。

http://www.astaro.com/lists/Web_Templates.zip

4.8.3.2 カスタム Web テンプレートと画像のアップロード

カスタムテンプレートの編集と保存ができたら、それをUTMにアップロードできます。

Web テンプレートや画像をアップロードするには、以下の手順に従います。

1. **「*ファイルのアップロード*」ダイアログボックスを開きます。**
   アップロードするテンプレート種類の名前の横にあるフォルダアイコンをクリックするか、画像をアップロードする場合は「*画像*」の横にあるフォルダアイコンをクリックします。

   注 – 対応しているファイルの種類は `.png`、`.jpg`、`.jpeg`、および `.gif` です。

   「*ファイルのアップロード*」ダイアログボックスが開きます。

2. **テンプレートまたは画像を選択します。**
   アップロードするテンプレートまたは画像がある場所までブラウズします。

   テンプレートまたは画像を選択し、「*アップロード開始*」をクリックします。

   「*ファイルのアップロード*」ダイアログボックスが閉じます。

3. **「*適用*」をクリックします。**
   テンプレートまたは画像がアップロードされます。

4.8.4 メールメッセージ

Sophos UTMの SMTP/POP3 プロキシによって生成されるユーザメッセージに表示されるテキストをカスタマイズします。これらのメッセージを他の言語に翻訳したり、顧客サポートの連絡先情報が表示されるように変更したりできます。次のメッセージをカスタマイズできます。

- **隔離メッセージのリリース完了:**このメッセージは、メールが隔離から正常にリリースされたときに表示されます。
- **隔離メッセージリリース中のエラー:**このメッセージは、メッセージを隔離からリリースする際にエラーが発生したときに表示されます。
- **ブロックされた POP3 メール:**このメッセージは、POP3 メールがブロックされたときに受信者に送信されます。

Figure 16 カスタマイズ:POP3 プロキシのブロックメッセージ

4.9 SNMP

簡易ネットワーク管理プロトコル(SNMP)は、ルータ、サーバ、スイッチなどのネットワークに接続されたデバイスを監視するためにネットワーク管理システムで使用されます。SNMP によって管理者は、監視している各ネットワークデバイスの状態に関するクエリを速やかに実行できます。Sophos UTMは、SNMP クエリに返答したり、SNMP トラップを SNMP 管理ツールに送信するように設定できます。前者は「*管理情報ベース (MIB)*」によって実現します。MIB は、どのネットワークデバイスに対してどの情報がクエリ可能かを指定します。Sophos UTMは、SNMP バージョン 2 と 3 および以下の MIB をサポートしています。

- **DISMAN-EVENT-MIB:**イベント管理情報ベース
- **HOST-RESOURCES-MIB:**ホストリソース管理情報ベース
- **IF-MIB:**インタフェースグループ管理情報ベース
- **IP-FORWARD-MIB:**IPフォワーディングテーブル管理情報ベース
- **IP-MIB:***インターネットプロトコル*(IP)用管理情報ベース
- **NOTIFICATION-LOG-MIB:**通知ログ管理情報ベース
- **RFC1213-MIB:**TCP/IP ベースのインターネットのネットワーク管理用管理情報ベース:MIB II

- **SNMPv2-MIB:***簡易ネットワーク管理プロトコル*(SNMP)用管理情報ベース
- **TCP-MIB:***伝送制御プロトコル*(TCP)用管理情報ベース
- **UDP-MIB:***ユーザデータグラムプロトコル*(UDP)用管理情報ベース

Sophos UTMシステム情報を取得するには、最低でもRFC1213-MIB(MIB II)をコンパイルしたSNMP マネージャを使用する必要があります。

4.9.1 クエリ

「*マネジメント > SNMP > クエリ*」ページでは、SNMP クエリの使用を有効にできます。

SNMP クエリを設定するには、次の手順に従ってください。

1. **「*SNMP クエリ*」を有効にします。**
   トグルスイッチをクリックします。

   「*SNMP バージョン*」および「*SNMP アクセスコントロール*」セクションが編集可能になります。

2. **SNMP バージョンを選択します。**
   「*SNMP バージョン*」セクションで、ドロップダウンリストからバージョンを選択します。SNMP バージョン 3 には認証が必要です。

3. **許可されるネットワークを選択します。**
   「*許可ネットワーク*」ボックスにリストされているネットワークは、Sophos UTM上で実行されている SNMP エージェントにクエリを行うことができます。アクセスは常に読み取り専用です。

   - **コミュニティ名:**バージョン 2 を使用する場合、コミュニティ名を入力します。SNMP コミュニティ名はパスワードとして機能し、SNMP エージェントへのアクセスを保護します。デフォルトでは、SNMP コミュニティ名は "public" に設定されていますが、お客様のニーズに応じて変更できます。

     注 – コミュニティ名に使用できる文字:(a-z)、(A-Z)、(0-9)、(+)、( )、(@)、(.)、(-)、(空白)

   - **ユーザ名/パスワード:**バージョン 3 を使用する場合、認証が必要です。ユーザ名とパスワード(確認のために 2回)を入力し、リモート管理者がクエリを送信できるようにします。パスワードは 8文字以上にする必要があります。SNMP v3 では、認証に SHA を、暗号化に AES を使用します。ユーザ名とパスワードはその両方で使用されます。

4. **「*適用*」をクリックします。**
   設定が保存されます。

さらに、UTMについての追加情報を入力できます。

デバイス情報

「*デバイス情報*」テキストボックスに、名前、場所、管理者など、UTMに関する追加情報を指定できます。この情報は、SNMP 管理ツールが読み取って、UTMの識別に使用します。

注 – UTMと*許可ネットワーク*間のすべての SNMP トラフィック（プロトコルバージョン 2）は暗号化されず、パブリックネットワーク上での転送中に読むことができます。

Sophos UTM 通知 MIB

このセクションで、Sophos UTM notifier MIBをダウンロードできます。これには、通知トラップの現在の設定に基づいたSophos UTM SNMP 通知の定義が含まれます。

4.9.2 トラップ

「*トラップ*」タブで、UTMで発生した関連イベントの通知を SNMP トラップとして送信する宛先の SNMP トラップサーバを定義できます。これらのトラップを表示するには、特別な SNMP モニタリングソフトウェアが必要です。

SNMP トラップとして送られるメッセージには、オブジェクト識別子（OID）が含まれます。たとえば、`.1.3.6.1.4.1.9789` が挙げられます。これは、IANA が発行した私企業番号に属します。`.1.3.6.1.4.1` は `iso.org.dod.internet.private.enterprise` プレフィックスで、`9789` は Astaro の*私企業番号*です。通知イベントの OID は `1500` で、それに通知タイプの OID および対応するエラーコード（`000-999`）が追加されます。以下の通知タイプを使用できます。

- `DEBUG = 0`
- `INFO = 1`
- `WARN = 2`
- `CRIT = 3`

例:通知「INFO–302: 新しいファームウェア Up2Date がインストールされました（New firmware Up2Date installed）」では、OID `.1.3.6.1.4.1.9789.1500.1.302` を使用し、以下の文字列が割り当てられます。

```
[<HOST>][INFO][302]
```

`<HOST>` はプレースホルダでシステムのホスト名を表し、通知の件名フィールドのタイプおよびエラーコードのみが伝送されます。

SNMP トラップサーバを選択するには、以下の手順に従います。

1. **「*新規 SNMP トラップシンク*」をクリックします。**
   「*新規 SNMP トラップシンクの作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   ホスト:SNMP トラップサーバのホスト定義。

   コミュニティ名:SNMP コミュニティ名はパスワードとして機能し、クエリを行う SNMP メッセージへのアクセスを保護します。デフォルトでは、SNMP コミュニティ名は "public" に設定されています。それをリモート SNMP トラップサーバで設定された文字列に変更します。

   注 – コミュニティ名に使用できる文字:(a–z)、(A–Z)、(0–9)、(+)、( )、(@)、(.)、(–)、(空白)

   コメント(任意):説明などの情報を追加します。
3. **「*保存*」をクリックします。**
   新しい SNMP トラップサーバが「トラップ」タブに表示されます。

4.10 集中管理(HA)

「*集中管理*」メニューのページを使用すると、ゲートウェイのモニタリングやリモート管理に使用できる管理ツールへのインタフェースを設定することができます。

4.10.1 Sophos UTM Manager

Sophos UTM Manager (SUM) は、Sophosの一元 (集中) 管理用製品です。複数の UTM アプライアンスを SUM に接続して、一元的にモニタリング、設定、メンテナンスができます。

このタブでは、UTMを 1つまたは 2つの SUM へ接続する際の設定ができます。

注 – MSP ライセンスを使用している場合、SUM の無効化、SUM ホストの変更、また SUM 管理者の権限変更は、Sophos UTM Manager (SUM) でのみ実行できます。

Sophos UTMが SUM サーバのモニタリング対象とされるよう準備するには、次の手順に従ってください。

1. **「*Sophos UTM Manager*」タブで、SUM を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*SUM 設定*」エリアが編集可能になります。

2. **「*SUM ホスト*」を指定します。**
   UTM の接続先とする SUM サーバを選択または追加します。

   - **認証**(任意):SUM サーバで認証が必要な場合、このオプションを選択して、SUM サーバで設定したものと同じパスワード(共有シークレット)を入力します。
   - **SUM サーバを Up2Date キャッシュとして使用**(任意):Up2Date パッケージは、SUM サーバにあるキャッシュから取得することができます。ゲートウェイ用にこの機能を使用するには、「*SUM サーバを Up2Date キャッシュとして使用*」オプションを選択します。管理している SUM サーバで、Up2Date キャッシュ機能を適切に有効にしていることを確認してください。Up2Date キャッシュは、UpDates の親プロキシ設定と同時に使用できないことに注意してください。

3. **SUM の管理者の権限を定義します。**
   SUM で管理者は、管理を許された UTM の特定のエリアのみ管理することができます。ここでリストされている権限は、SUM ゲートウェイマネージャのメインメニューおよび権限オプションと一致します。

   管理者:選択すると、管理者は、「*メンテナンス*」と「*管理*」メニューにあるすべてての機能を利用することができます。たとえば、リストの表示、バックアップの作成とリストア、ファームウェアアップデートのスケジュール設定などです。

   レポート:選択すると、管理者は、「*レポート*」メニューにあるすべての機能を利用することができます。たとえば、UTM からレポートを要求できます。

   監視:選択すると、「*監視*」ページに UTM が表示され、管理者は関連する機能すべてを利用することができます。

   設定:選択すると、管理者は、「*設定*」メニューにあるすべての機能を利用することができます。たとえば、ネットワーク、ホスト、VPN などのオブジェクトを UTM にデプロイできます。

   注 – 詳細は、「Sophos UTM Manager 管理ガイド」を参照して下さい。

4. **「*適用*」をクリックします。**
   設定が保存されます。

   UTM は Sophos UTM Manager と接続を確立しようとします。両システム間の接続が確立したら、接続ステータスは緑色に変わります。以後、ここで選択した SUM サーバで UTM をモニタリングおよび管理できるようになります。「*SUM のステータス*」セクションで、現在の接続ステータスと健全性を確認することができます。ページをリロードすると、このデータが更新されます。接続に関する問題が発生した場合は、「*ライブログを開く*」ボタンを使用し、掲示板のメッセージを参照して問題を診断してください。

2台目の SUM の設定

このセクションでは、2台目の SUM を任意に追加することができます。これは、例えばご自分で設定を行い(1台目の SUM サーバ)、かつ第三者、例えば MSSP によるモニタを必要とする場合(2台目の SUM サーバ)などに有効です。この設定は 1台目の SUM サーバとほぼ同様です。ただし、*設定*のオプションは 1台目の SUM サーバに限られているため、2台目では設定できません。

注 – ゲートウェイと SUM の間の通信はポート `4433` で行われますが、Sophos UTM Manager には、HTTPS プロトコルを使用してブラウザ経由でアクセスすることができます。WebAdmin の場合はポート `4444`、ゲートウェイマネージャインタフェースの場合はポート `4422` です。

SUMのステータス

「*SUMのステータス*」セクションで、現在の接続ステータスと健全性を確認することができます。ページをリロードすると、このデータが更新されます。

SUM オブジェクト

このエリアは、SUM 経由で作成されたオブジェクトがあり、この SUM がSophos UTMから切断されている場合を除き、無効になっています(グレーアウト表示されています)。SUM で作成されたオブジェクトとは、ネットワーク定義、リモートホスト定義、IPsec VPNトンネルなどです。

「*オブジェクトのクリーンアップ*」ボタンを押すと、デバイスを以前に管理していた SUM で作成されたすべてのオブジェクトをリリースすることができます。これらのオブジェクトは通常ロックされ、ローカルデバイスのみで表示できます。このボタンを押すと、オブジェクトは完全にアクセス可能になり、ローカル管理者が再利用または削除できます。

注 – 以前に SUM で作成されたオブジェクトをクリーンアップすると、同じ SUM に再接続したときにこれらのオブジェクトを再変換できなくなります。つまりリモートの SUM が、後で接続を再確立するデバイス用にオブジェクト定義をまだホストしている場合、ローカルコピーがすでに存在しても、これらのオブジェクトはデバイスに再配備されます。

ライブログ

ライブログを使用して、Sophos UTMと SUM の間の接続をモニタリングすることができます。クリック*ライブログ*ライブログを新しいウインドウで開くためのボタン。

4.11 冗長化(HA)

インターネットセキュリティシステムの障害の主な原因は、ハードウェアの故障です。システムに障害が発生した後もサービスを継続して提供する能力をフェイルオーバと呼びます。Sophos UTMはHA フェイルオーバを実現するため、お客様はプライマリシステムで障害が発生したときのためにホットスタンバイシステムをセットアップできます(active-passive)。あるいは、Sophos UTMを使用してクラスタをセットアップして、専用のネットワークトラフィックを一群のノードに分散させて運用し(active-active)、リソース利用率を最大限に高めて処理時間を削減することができます。これは従来のロードバランシングアプローチと似ています。

Sophos UTMに導入された「*冗長化*」と「*クラスタ*」の概念は、緊密に連携しています。HA システムは2ノードクラスタと考えることができます。これは冗長性を実現する最低限の要件です。

クラスタ内の各ノードは次のいずれかの役割を果たすことができます。

- **マスタ:**ホットスタンバイ/クラスタセットアップ上のプライマリシステム。クラスタ内で、マスタはデータの同期と配信を行う責任を担います。
- **スレーブ:**ホットスタンバイ/クラスタセットアップ内のスタンバイシステム。マスタに障害が発生すると、オペレーションを引き継ぎます。
- **ワーカー:**データ処理のみを担当するシンプルなクラスタノード。

すべてのノードは、いわゆるハートビート信号を使用して自らをモニタリングします。ハートビート信号とは、他のノードが稼働していることを確認するために定期的に送信されるマルチキャスト UDP パケットです。技術的エラーが原因で、いずれかのノードがこのパケットの送信に失敗すると、そのノードは *デッド(Dead)* と宣言されます。失敗したノードが担っていた役割に応じて、セットアップの構成が次のように変更されます。

- マスタノードで障害が発生した場合、スレーブがマスタの役割を引き継ぎ、IDが最も高いワーカノードがスレーブとなります。
- スレーブノードで障害が発生した場合、IDが最も高いワーカノードがスレーブとなります。
- ワーカノードで障害が発生した場合、処理能力が失われることによるパフォーマンス低下は認識されますが、フェイルオーバー機能は損なわれません。

レポーティング

すべてのレポーティングデータはマスタノード上で統合され、5分間隔で他のクラスタノードと同期されます。したがって、引き継ぎが発生すると、最大過去5分間のレポーティングデータが失われま

す。ただし、データ収集プロセスには違いがあります。「*ログとレポート > ハードウェア*」タブに表示されるグラフには、現在マスタとなっているノードのデータのみが表示されます。一方、「*ログとレポート > ネットワーク使用状況*」ページなどに表示されるアカウンティング情報には、関連するすべてのノードから収集されたデータが表示されます。たとえば、今日の CPU 使用状況のヒストグラムには、マスタノードの現在のプロセッサ使用状況が表示されます。切り替わりが発生した場合、ここにはスレーブノードのデータが表示されるようになります。一方、上位アカウンティングサービスに関する情報などは、ユニットを通過するトラフィックの分散処理に関与したすべてのノードから収集されたデータの集合体となります。

注記

- *アドレス解決プロトコル*(ARP)を使用するのは、実際のマスタのみです。つまり、スレーブノードとワーカノードはARP要求の送信や応答を行いません。
- フェイルオーバが発生すると、オペレーションを引き継ぐユニットが ARP アナウンスメント(別名「*gratuitous ARP*」)を実行します。これは通常、要求を受信する他のホストの ARP キャッシュを更新することを目的とするARP要求です。Gratuitous ARP は、マスタの IP がスレーブに移行したことをアナウンスするために使用されます。
- マスタで設定するすべてのインタフェースには物理リンクが必要です。つまり、任意のネットワークデバイスにポートを正しく接続しなければなりません。

4.11.1 ハードウェアとソフトウェアの要件

HA フェイルオーバまたはクラスタ機能を提供するためには、次のハードウェアおよびソフトウェア要件を満たす必要があります。

- 冗長化オプションが使用可能な有効なライセンス(スタンバイユニットの場合、追加の基本ライセンスのみが必要です)。
- ソフトウェアバージョンとハードウェアが同じである2台のUTMユニット、または同じモデルの2台のUTMアプライアンス。
- ハートビートが可能なイーサネットネットワークカード。サポートされているネットワークカードを確認するには、HCL をチェックしてください。HCL はSophos サポートデータベースで提供されています(検索用語に「HCL」を使用します)。
- イーサネットクロスオーバーケーブル(ホットスタンバイシステムでのマスタとスレーブの接続用)。UTM専用 HA インタフェースがギガビット自動 MDX デバイスであるアプライアンスのモデル 320、425、525 は、標準の IEEE 802.3 イーサネットケーブルで接続可能です(イーサネッ

トポートが送信/受信ペアを自動的に交換するため)。

- ネットワークスイッチ(クラスタノードの接続用)。

4.11.2 ステータス

「*マネジメント > 冗長化 > ステータス*」タブには、ホットスタンバイシステムまたはクラスタに関与するすべてのデバイスがリストされ、次の情報が表示されます。

- **ID:**デバイスのノード ID。ホットスタンバイシステムでは、ノード ID は 1(マスタ)または 2(スレーブ)です。
  クラスタ内のノード ID は 1～10 の範囲になります。この理由は、1つのクラスタに最大 10 ノードまで持たせることができるためです。
- **役割:**クラスタ内の各ノードは次のいずれかの役割を果たすことができます。
  - MASTER:ホットスタンバイ/クラスタセットアップ上のプライマリシステム。クラスタ内でデータの同期と配信を行う責任を担います。
  - SLAVE:ホットスタンバイ/クラスタセットアップ内のスタンバイシステム。マスタに障害が発生すると、オペレーションを引き継ぎます。
  - WORKER:データ処理のみを担当するシンプルなクラスタノード。
- **デバイス名:**デバイスの名前です。
- **ステータス:**HA ステータスに関するデバイスの状態。次のいずれかになります。
  - ACTIVE:ノードは完全に機能しています。
  - UNLINKED:1つ以上のインタフェースリンクがダウンしています。
  - UP2DATE:Up2Date が進行中です。
  - UP2DATE FAILED:Up2Date が失敗しました。
  - DEAD:ノードに到達できません。
  - SYNCING:データ同期が進行中です。このステータスは、引き継ぎプロセスの進行中に表示されます。最初の同期には 5分以上時間がかかります。あらゆる同期関連のプログラムにより、この時間が長期化する場合もあります。スレーブが同期中であり「*同期中*」ステータスの場合、マスタノードでのリンク障害などが原因で正常な引き継ぎは行われません。
- **バージョン:**システムにインストールされたSophos UTMソフトウェアのバージョン番号。
- **最後のステータス変化:**ステータス変更が最後に発生した時間。

リブート/シャットダウン:これらのボタンを使用して、デバイスを手動でリブートまたはシャットダウンすることができます。

ノード削除:このボタンを使用して、WebAdmin 経由でデッド状態のクラスタノードを削除します。メール隔離やスプールなど、ノード固有のすべてのデータがマスタに引き継がれます。

HA ライブログを別ウィンドウで表示するには、右上隅にある「*HA ライブログを開く*」ボタンをクリックします。

4.11.3 システムステータス

「*マネジメント > 冗長化 > システムステータス*」タブには、ホットスタンバイシステムまたはクラスタに関与するすべてのデバイスがリストされ、各デバイスのリソース使用状況に関する次の情報が表示されます。

- CPU 使用率 (%)
- RAM 使用率 (%)
- スワップ使用率 (%)
- ログパーティションで消費されているハードディスクの容量 (%)
- ルートパーティションで消費されているハードディスクの容量 (%)
- UPS(無停電電源装置)モジュールがある場合はその状況

4.11.4 設定

Sophos UTMの冗長化機能は、3つの基本設定をカバーします。

- 自動設定
- ホットスタンバイ (active–passive)
- クラスタ (active–active)

自動設定: Sophos UTMSophos UTM には、UTMアプライアンス用のプラグアンドプレイ設定オプションがあります。このオプションを使用すると、クラスタに追加するデバイスを再設定したり手動でインストールしたりする必要なく、ホットスタンバイシステム/クラスタをセットアップすることができます。UTMアプライアンスの専用 HA インタフェース (`eth3`)を相互に接続し、すべてのデバイスで「*自動設定*」を選択するだけで、準備は完了です。

注 – *自動設定*が正常に機能するためには、すべてのUTMアプライアンスは同じモデルでなければなりません。たとえば、HAシステムのセットアップには、2台のUTM 320アプライアンスを使用する必要があり、UTM 220ユニットとUTM 320ユニットを組み合わせて使用することはできません。

この専用インタフェースを介して 2台のUTMアプライアンスを接続すると、すべてのデバイスが相互に認識し、HA システムとして自動的に自己設定します。アップタイムが長い方のデバイスがマスタとなります。可能性は低いものの、アップタイムが同じであった場合には、MAC アドレスに基づいてマスタとなるデバイスが決まります。

UTMソフトウェアを使用すると、専用スレーブシステムで「*自動設定*」オプションが使用され、マスタまたはすでに設定されているホットスタンバイシステム/クラスタに自動的に追加されます。このため、「*自動設定*」は、それ自体、冗長化オペレーションモードではなく移行モードと考えることができます。「*自動設定*」が選択されているデバイスがホットスタンバイシステムまたはクラスタに追加されると、冗長化オペレーションモードはそれぞれ「*ホットスタンバイ*」または「*クラスタ*」となります。ただし、この機能が正常に機能するためには、マスタシステムで「*新規デバイスの自動設定を許可*」オプションが有効になっていることが条件となります。この機能により、冗長化オペレーションモードが「*自動設定*」に設定されているデバイスがホットスタンバイシステム/クラスタに自動的に追加されます。

ホットスタンバイ (active-passive): Sophos UTMSophos UTM では、2つのノードから成るホットスタンバイ冗長化コンセプトが採用されており、冗長性を実現する最低要件となります。Sophos UTMソフトウェア9に導入された主な改良点の1つに、テイクオーバー(引き継ぎ)のレイテンシを 2秒未満に低減できる点があります。ゲートウェイは、ファイアウォール接続の同期化に加え、IPsecトンネルの同期化にも対応してます。つまり、ロードウォリアやリモート VPN ゲートウェイが、テイクオーバー後にIPsecトンネルを再度確立する必要はありません。また、隔離されたオブジェクトも同期化されるため、テイクオーバー後も使用可能です。

クラスタ (active-active):(ベーシックガードサブスクリプションでは、利用できません。)大量のインターネットトラフィックのリアルタイム処理に対する需要が高まっています。これに対応するために、Sophos UTMには、処理集約型のタスク(コンテンツフィルタ、ウイルススキャン、侵入防止、復号化など)を複数のクラスタノードに均一に分散するためのクラスタリング機能が用意されています。専用のハードウェアベースの負荷分散装置を使用する必要なく、ゲートウェイの全体的なパフォーマンスを大幅に向上できます。

注 – クラスタの設定時は、マスタノードを設定してから残りのユニットをスイッチに接続してください。

マスタ、スレーブ、またはワーカの設定手順は非常に似ています。次の手順で実行します。

1. **冗長化オペレーションモードを選択します。**
   デフォルトでは、冗長化はオフになっています。次のモードを使用できます。

   - 自動設定
   - ホットスタンバイ(active-passive)
   - クラスタ(active-active)

   注 – 冗長化オペレーションモードを変更する場合、モードを「*自動設定*」、「*ホットスタンバイ*」、または「*クラスタ*」に変更するためには、モードを一度「*OFF*」に戻す必要があります。

   選択に応じて、1つ以上のオプションが表示されます。

2. **次の設定を行います。**
   同期用 NIC:マスタシステムとスレーブシステムとの通信で経由するネットワークインタフェースカードを選択します。リンクアグリゲーションがアクティブである場合、ここでリンクアグリゲーションインタフェースも選択できます。

   注 – まだ設定していないインタフェースのみが表示されます。実行中の設定で同期化インタフェースを変更することができます。その後、すべてのノードはリブートします。

   次のオプションは、オペレーションモードとして「*ホットスタンバイ*」または「*クラスタ*」を選択した場合のみ設定できます。

   デバイス名:このデバイスを説明する名前を入力します。

   デバイスノード ID:デバイスのノード ID を選択します。プライマリシステムに障害が発生した場合、ID が最も高いノードがマスタとなります。

   暗号化キー:マスタとスレーブの通信を暗号化するパスフレーズ(確認のためにパスフレードを 2回入力します)。鍵の最大長は 16文字です。

3. **「*適用*」をクリックします。**
   デバイスで冗長化フェイルオーバーがアクティブになりました。

ホットスタンバイモードのゲートウェイは、データ転送接続に対して定期的に更新されます。アクティブなプライマリシステムでエラーが発生した場合、速やかにセカンダリシステムが通常モードに自動的に切り替わり、プライマリシステムの機能を引き継ぎます。

注 – ホットスタンバイシステム/クラスタを無効にすると、スレーブノードとワーカノードは工場出荷時の状態に戻り、シャットダウンします。

詳細情報(特に使用事例)は、Sophosサポートデータベースにある「*HA/クラスタガイド*」で確認できます。

詳細

このセクションでは、詳細設定を行うことができます。

新規デバイスの自動設定を許可:ホットスタンバイシステム/クラスタを手動で設定した場合、このオプションにより、冗長化オペレーションモードが「*自動設定*」に設定されているデバイスがホットスタンバイシステム/クラスタに自動的に追加されます。ただし、このオプションはスレーブシステムに一切影響を与えないため、デフォルト設定のまま有効にしておくことができます。

Up2Date 時にノードをそのまま保持:選択する場合、新しいシステムバージョンへの更新時に、HA/クラスタノードの半数が現在のシステムバージョンを保持します。新しいバージョンが安定した段階で、「*マネジメント > 冗長化 > ステータス*」ページで残りのノードを更新できます。新しいバージョンのために更新されたすべてのノードで障害が発生する場合は、残りのノードが古いバージョンで新しい HA/クラスタを構築します。その後、障害のあるノードに古いバージョンをインストールするか、新しい更新を待つことができます。

「*Up2Date 時にノードをそのまま保持*」を有効にすると、同期は同じシステムバージョンを持つノードにしか適用されないため、バージョン保持を選択したノードはアップデート後同期されなくなります。その代わり、保持を選択したノードの状態は維持されます。このため、何らかの理由で、保持したノードを再アクティベーションする場合、アップデート開始時から再アクティベーションするまでの間に発生した設定の変更やレポートデータは失われます。

優先マスタ:ここでは、ドロップダウンリストでノードを選択して、指定のマスタノードを定義できます。フェイルオーバーが発生した場合、選択されたノードはリンクの回復後はスレーブモードのままではなく、マスタモードにスイッチバックします。

バックアップインタフェース:HA 同期化インタフェースの障害やネットワークケーブルの切断などが原因で、マスタとスレーブの両方が同時にマスタになること(マスタ/マスタの状況)を防ぐために、バックアップ用のハートビートインタフェースを選択できます。この追加ハートビートインタフェースには、いずれかの設定済みアクティブイーサネットインタフェースを選択できます。バックアップインタフェースを選択すると、マスタ/スレーブ設定が維持されていることを確認するために、このインタフェース経由で追加のハートビート信号が一方向へ(マスタからスレーブへ)送信されます。マスタ/スレーブ接続が無効であり、バックアップインタフェースが関与すると、いずれかのクラスタノードが停止していることを知らせる通知が管理者に送信されます。ただし、このオプションはスレーブシステムに一切影響を与えないため、未設定のままにしておくことができます。

注 – HA 同期化インタフェースに障害が発生した場合、設定はそれ以上同期されなくなります。バックアップインタフェースは、マスタ/マスタの状況を回避するだけです。

4.12 シャットダウンとリスタート

このタブでは、手動でSophos UTMをシャットダウンまたはリスタートできます。

シャットダウン:この操作により、システムをシャットダウンして、すべてのサービスを適切に停止できます。モニタや LCD ディスプレイが接続されていないシステムの場合は、シャットダウンプロセスの最後にビープ音が 1秒間隔で鳴り続けます。

Sophos UTMをシャットダウンするには、以下の手順に従います。

1. **「*システムをシャットダウン(停止)*」をクリックします。**
2. **警告メッセージを確認します。**
   「システムをシャットダウンしますか？」というメッセージが表示されたら、「*OK*」をクリックします。

   システムはシャットダウンして停止します。

お使いのハードウェアおよび設定により、シャットダウンが完了するまでに数分かかる場合があります。システムが完全にシャットダウンした後で、電源を切ります。システムが完全にシャットダウンする前に電源を切ると、システムが次回の起動(ブート)時にファイルシステムの一貫性をチェックするため、起動プロセスに通常よりかなり長く時間がかかることになります。最悪の場合は、データが失われる場合があります。

システムの起動が正常に行われるとビープ音が連続して 5回鳴ります。

リスタート:この操作により、システムを完全にシャットダウンして再起動します。お使いのハードウェアおよび設定により、完全にリスタートするまでに数分かかる場合があります。

Sophos UTMをリスタートするには、次の手順に従います。

1. **「*システムをリスタート(リブート)*」をクリックします。**
2. **警告メッセージを確認します。**
   「システムをリスタートしますか？」というメッセージが表示されたら、「*OK*」をクリックします。

   システムはシャットダウンし、停止してからリブートします。

5 定義とユーザ

この章では、Sophos UTM全体で使用されるネットワーク、サービス、期間の定義を設定する方法について説明します。WebAdmin の「*オブジェクト定義の概要*」ページは、タイプに基づくネットワーク定義の数と、プロトコルタイプに基づくサービス定義の数を示します。

「*定義とユーザ*」メニューのページを使用すると、他のすべての設定メニューで使用することが可能なネットワークとサービスを一元的に定義することができます。これにより、IP アドレス、ポート、ネットワークマスクなどに悩まされることなく、名前を使用して作業できます。その他のメリットとしては、個々のネットワークやサービスをグループにまとめて、一度に設定できることがあげられます。後でこれらのグループに特定の設定を割り当てたりすると、これらの設定はグループに含まれるすべてのネットワークとサービスに適用されます。

さらに、この章では、Sophos UTMのユーザアカウント、ユーザグループ、および外部認証サーバの設定方法や、クライアント PC の認証について説明します。

この章では、次のトピックについて説明します。

- ネットワーク定義
- サービス定義
- 時間帯定義
- ユーザとグループ
- クライアント認証
- 認証サーバ

5.1 ネットワーク定義

*「定義とユーザ」>「ネットワーク定義」*メニューでは、ホスト、ネットワーク、ネットワークグループ、また MAC アドレスの定義を作成できます。ここで作成した定義は、他の多くの WebAdmin 設定でも使用できます。

5.1.1 ネットワーク定義

「*定義とユーザ > ネットワーク定義 > ネットワーク定義*」タブは、UTMのホスト、ネットワーク、ネットワークグループを一元的に定義する場所です。ここで作成した定義は、他の多くの WebAdmin 設定メニューでも使用できます。

デフォルトでは、タブを開くとすべてのネットワーク定義が表示されます。リストの上部のドロップダウンリストを使用して、特定のプロパティを持つネットワーク定義を表示するように選択できます。

ヒント – 「*ネットワーク定義*」リストでネットワーク定義の情報アイコンをクリックすると、ネットワーク定義が使用されているすべての設定項目を表示できます。

ネットワークテーブルには、システムが自動的に作成した、編集も削除もできないスタティックネットワークも含まれています。

- **インタフェースアドレス:**このタイプの定義は、各ネットワークインタフェースに追加されます。ここには、インタフェースの現在の IP アドレスが含まれています。名前では、インタフェース名の後に「(Address)」という言葉が付いています。
- **I/F ブロードキャストアドレス:**このタイプの定義は、各イーサネットタイプネットワークインタフェースに追加されます。ここには、インタフェースの現在の IPv4 ブロードキャストアドレスが含まれています。名前では、インタフェース名の後に「(Broadcast)」という言葉が付いています。
- **I/F ネットワークアドレス:**このタイプの定義は、各イーサネットタイプネットワークインタフェースに追加されます。ここには、インタフェースの現在の IPv4 ネットワークが含まれています。名前では、インタフェース名の後に「(Network)」という言葉が付いています。
- **インターネット (IPv4/IPv6):**インタフェースに関連付けられたネットワーク定義 (それぞれ IPv4、および IPv6 が有効な場合は IPv6用)。デフォルトゲートウェイとして機能します。設定でこれを使用すると、設定プロセスが容易になります。アップリンクバランシングを有効にすると、*インターネット*定義は*アップリンクインタフェース*と関連付けられます。

注 – クライアント認証で認証されたユーザネットワークオブジェクトは、パフォーマンス上の理由から常に未解決として表示されます。

ネットワーク定義を作成するには、次の手順に従います。

1. **「*ネットワーク定義*」タブで、「*新規ネットワーク定義*」をクリックします。**
   「*新規ネットワーク定義の作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   (選択した定義タイプに応じて、ネットワーク定義のさらに詳細なパラメータが表示されます。)

   名前:この定義を説明する名前を入力します。

   タイプ:ネットワーク定義タイプを選択します。次のタイプを使用できます。

- **ホスト:**単一 IP アドレス。次の情報を指定します。
  - **IPv4 アドレス/IPv6 アドレス:**ホストの IP アドレス (設定されたインタフェースの IP アドレスを入力することはできません)。
  - **DHCP 設定** (オプション):このセクションでは、ホストと IP アドレス間のスタティックマッピングを作成できます。これには、設定された DHCP サーバが必要になります(「*ネットワークサービス > DHCP > サーバ*」参照)。

    注 – DHCP プールから通常通りに割り当てられたアドレスとスタティックにマッピングされたアドレスの間でIPアドレスの重複が発生することを防止するために、スタティックにマッピングする場合はDHCPプールの範囲外のアドレスを指定してください。たとえば、DHCP プールが `192.168.0.100`〜`192.168.0.210` である場合にスタティックマッピングとして `192.168.0.200` を指定すると、2つのシステムが同じ IP アドレスを持つことになります。

    IPv4 DHCP:スタティックマッピングに使用する IPv4 DHCP サーバを選択します。

    MAC アドレス:ホストのネットワークインタフェースカードの MAC アドレスを入力します。MAC アドレスは通常、2桁の 16進数をコロンで区切って6組まとめた形式で指定します(`00:04:76:16:EA:62`など)。

    IPv6 DHCP:スタティックマッピングに使用する IPv6 DHCP サーバを選択します。

    DHCP 個別識別子:ホストの DUID を入力します。Windows などの OS の場合、次の Windows レジストリで DUID を確認できます。
    `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\TCPIP6\Parameters`

    2桁の 16進数をコロンで区切ってまとめた形式で指定します(`00:01:00:01:13:30:65:56:00:50:56:b2:07:51` など)。
  - **DNS 設定** (オプション):独自の DNS サーバをセットアップせず、ネットワーク内のいくつかのホストに対してスタティック DNS マッピングが必要な場合は、該当するホストのこのセクションでこれらのマッピングを入力することができます。これは限られた数のホストにしか対応できないため、フルオペレーションを行っている DNS サーバの代わりに使用することは決してしないでください。

ホスト名:ホストの FQDN（完全修飾ドメイン名）を入力します。

リバース DNS:ホストの IP アドレスと名前のマッピングを有効化するには、チェックボックスにチェックを入れます。同じ IP アドレスに複数の名前をマッピングすることが可能ですが、1つの IP アドレスには1つの名前にしかマッピングできません。

追加ホスト名:ホストにホスト名を追加するには、プラスアイコンをクリックします。

- **DNS ホスト:**DNS ホスト名。システムによってダイナミックに解決され、IP アドレスが生成されます。DNS ホストは、ダイナミック IP エンドポイントの使用時に便利です。システムは、TTL（生存時間）の値に従って定期的にこれらの定義を再解決し、新しい IP アドレスがある場合は定義を更新します。次の情報を指定します。
  - **ホスト名:**リゾルブしたいホスト名。
- **DNS グループ:**DNS ホストと似ていますが、1つのホスト名用の DNS 内の複数の RR（リソースレコード）を処理できます。透過プロキシでのファイアウォールルールと除外の定義に便利です。
- **ネットワーク:**標準的な IP ネットワーク。ネットワークアドレスとネットマスクから構成されています。次の情報を指定します。
  - **IPv4 アドレス/IPv6 アドレス:**ネットワークのネットワークアドレス（設定されたインタフェースの IP アドレスを入力することはできません）。
  - **ネットマスク:**オクテット内のいくつのビットでサブネットワークが指定され、いくつのビットがホストアドレスに使用されるかを示すために使用されるビットマスク。
- **レンジ:**IPv4 アドレスレンジの全範囲を定義するために選択します。次の情報を指定します。
  - **IPv4 先頭:**レンジの先頭の IPv4 アドレス。
  - **IPv4 末尾:**レンジの末尾の IPv4 アドレス。
- **マルチキャストグループ:**定義されたマルチキャストネットワーク範囲から構成されるネットワーク。
  - **IPv4 アドレス:**マルチキャストネットワークのネットワークアドレス。`224.0.0.0`〜`239.255.255.255` の範囲である必要があります。
  - **ネットマスク:**オクテット内のいくつのビットでサブネットワークが指定され、いくつのビットがホストアドレスに使用されるかを示すために使用されるビットマスク。

- **ネットワークグループ:**他のネットワーク定義リストを含むコンテナ。これらを使用してネットワークとホストをまとめると、設定がより読みやすくなります。「*ネットワークグループ*」を選択すると、「*メンバー*」ボックスが表示され、グループメンバーを追加できます。
- **アベイラビリティグループ:**ホストまたは DNS ホスト(あるいはその両方)のグループ。優先順位に基づいてソートされています。すべてのホストの生存ステータスが ICMP ping により、デフォルトで 60秒間隔でチェックされます。優先順位が最も高く、生存ステータスであるホストが設定で使用されます。「*アベイラビリティグループ*」を選択すると、「*メンバー*」ボックスが表示され、グループメンバーを追加できます。

コメント(任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
表示されるオプションは、上で選択されている「*タイプ*」に依存します。

インターフェース(任意):ネットワーク定義を特定インタフェースにバインドして、その定義への接続がこのインタフェース経由でのみ確立されるようにすることができます。

モニタリングタイプ(「*アベイラビリティグループ*」選択時のみ):生存ステータスチェックのサービスプロトコルを選択します。モニタリング用に「*TCP*」(TCP 接続の確立)、「*UDP*」(UDP 接続の確立)、「*Ping*」(ICMP Ping)、「*HTTP ホスト*」(HTTP 要求)、または「*HTTPS ホスト*」(HTTPS 要求)のいずれかを選択します。「*UDP*」を使用する場合、ping 要求が最初に送信され、成功した場合は、続いてペイロード 0 の UDP パケットが送信されます。ping が成功しなかった場合や、ICMP ポートに到達できない場合、このホストはダウンしているとみなされます。

ポート(「*TCP*」または「*UDP*」のモニタリングタイプ選択時のみ):要求の送信先のポート番号。

URL(オプション。「*HTTP ホスト*」または「*HTTPS ホスト*」のモニタリングタイプ選択時のみ):要求する URL。URL にポート情報を追加することで、デフォルトのポート 80 または 443 以外のポートを使用できます(例: `http://example.domain:8080/index.html`)。URL を指定しない場合は、ルートディレクトリが要求されます。

間隔:ホストをチェックする間隔を秒単位で入力します。

タイムアウト:ホストが応答を送信する最大時間を秒単位で入力します。ホストがこの時間内に応答しない場合、デッド(dead)とみなされます。

常にリゾルブ:このオプションはデフォルトで選択されているため、すべてのホストが使用不可である場合、グループは最後に使用可能であったホストで解決されます。

チェックを外すと、すべてのホストがデッド (dead) の場合は、グループが *未解決* に設定されます。

4. **「*保存*」をクリックします。**
   新しい定義がネットワーク定義リストに表示されます。

ネットワーク定義を編集または削除するには、対応するボタンをクリックします。

5.1.2 MAC アドレス定義

*「定義とユーザ」>「ネットワーク定義」>「MAC アドレス定義」*タブは、MAC アドレスリストなどの MAC アドレスの定義を一元的に設定する場所です。MAC アドレスの定義によって、ホストや IP アドレスに基づいたルールをさらに定義済みの MAC アドレスを持つデバイスにマッチするものだけに限定するために使用できます。

ヒント – 「MAC アドレス定義」の情報アイコンをクリックすると、この定義が使用されているすべての設定オプションを表示できます。

MAC アドレス定義を作成するには、以下の手順に従います。

1. **「*MAC アドレス定義*」タブで、「*新規 MAC アドレスリスト*」をクリックします。**
   「*MAC アドレスリストを作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前: この定義を説明する名前を入力します。

   MAC アドレス: プラスのアイコンをクリックして、各 MAC アドレスを続けて入力するか、アクションアイコンを使用してコピーアンドペーストにより MAC アドレスリストをインポートします。MAC アドレスは通常、2桁の 16進数をコロンで区切って6組まとめた形式で指定します (`00:04:76:16:EA:62` など)。

   ホスト: MAC アドレス定義に追加する MAC アドレスを持つホストを 追加します。ホスト定義の「*DHCP 設定*」セクションで定義された MAC アドレスが MAC アドレスリストに追加されます。

   注 – MAC アドレスまたはホストのどちらか一方または両方入力することができます。

   コメント (任意): 説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しい定義が「*MAC アドレス定義*」リストに表示されます。

MAC アドレス定義を編集あるいは削除するには、該当するボタンをクリックします。

5.2 サービス定義

「*定義とユーザ > サービス定義*」ページで、サービスおよびサービスグループを定義して一元管理できます。サービスは、特定タイプのネットワークトラフィックの定義で、TCP や UDP といったプロトコルに関する情報とプロトコル関連オプション（ポート番号など）に関する情報を組み合わせています。サービスを使用して、UTM で許可または拒否されるトラフィックのタイプを決定することができます。

ヒント –「*サービス定義*」リストのサービス定義の情報アイコンをクリックすると、サービス定義が使用されているすべての設定オプションを表示できます。

サービス定義を作成するには、以下の手順に従います。

1. **「*サービス定義*」ページで「*新規サービス定義*」をクリックします。**
   「*新規サービス定義の作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   （選択した定義タイプに応じて、サービス定義のさらに詳細なパラメータが表示されます。）

   名前:この定義を説明する名前を入力します。

   定義タイプ:サービスタイプを選択します。次のタイプを使用できます。

   - **TCP:**TCP 接続では、0 ～ 65535 のポート番号を使用します。ロストしたパケットは TCP が認識して再度リクエストします。TCP 接続では、受信者は送信者に対してデータパケットを受信したときに通知します（接続関連のプロトコル）。TCP セッションは 3WAY ハンドシェークで始まり、セッションの最後に接続がクローズします。次の情報を指定します。
     - **宛先ポート:**宛先ポートを単一のポート番号（例: 80）あるいは範囲（例: 1024:64000）として入力します。範囲を指定する場合は、コロンを区切り文字として使用します。
     - **送信元ポート:**送信元ポートを単一のポート番号（例: 80）あるいは範囲（例: 1024:64000）として入力します。範囲を指定する場合は、コロンを区切り文字として使用します。
   - **UDP:***UDP（User Datagram Protocol）*は、0 ～ 65535 のポート番号を使用するステートレスプロトコルです。UDP はステートを維持しないため、TCP より高速です。特に、少量のデータは高速に送信できます。ただし、このステートレスであるということ

は、UDP はパケットがロストまたはドロップした場合に認識できないことも意味します。受信コンピュータは、データパケットを受信しても送信者に通知しません。*UDP* を選択した場合は、TCP の場合と同じ設定オプションを編集できます。

- **TCP/UDP:**TCP と UDP の組み合わせで、DNS などの両方のサブプロトコルを使用するアプリケーションプロトコルに適切です。*TCP/UDP*を選択した場合は、TCP または UDP の場合と同じ設定オプションを編集できます。
- **ICMP/ICMPv6:**ICMP *(Internet Control Message Protocol)* は主にエラーメッセージの送信に使用されます。たとえば、要求されたサービスが利用できない、あるいはホストやルータに到達できなかった、などのメッセージを送信します。*ICMP* または *ICMPv6*を選択した場合は、ICMP コード/タイプを選択します。IPv4 ファイアウォールルールは ICMPv6 では機能せず、IPv6 ファイアウォールルールは ICMP では機能しません。
- **IP:**IP *(Internet Protocol)* は、インターネット上でのデータのやり取りに使用されるネットワークおよび伝送プロトコルです。*IP* を選択したら、IP 内でカプセル化されるプロトコルの番号を指定します(例: 121、これは SMP プロトコルを表します)。
- **ESP:**ESP *(カプセル化セキュリティペイロード)* は、IPsec トンネリングプロトコルスイートの一部で、VPN を介してトンネルされるデータに暗号化サービスを提供します。ESP または AH を選択した場合は、*SPI (セキュリティパラメータインデックス)*を指定します。これは、IP アドレスとともにセキュリティパラメータを特定します。特に自動 IPsec 鍵交換を使用する場合は、256～4,294,967,296 の値を入力するか、または 256～4,294,967,296 の範囲として指定されたデフォルト設定を使用します(コロンを区切り文字として使用します)。1～255 の番号は *IANA (Internet Assigned Numbers Authority)*によって予約されています。
- **AH:***認証*ヘッダー(AH) は IPsec トンネリングプロトコルスイートの一部で、IP ヘッダとデータグラムペイロード間に位置し、情報の (機密性ではなく) 整合性を維持します。
- **グループ:**他のサービス定義リストを含むコンテナ。設定を読みやすくするために、これらを使用してサービス定義をまとめることができます。「*グループ*」を選択すると、「メンバー」ボックスが開くので、そこでグループのメンバー(その他のサービス定義など)を追加します。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しい定義が「*サービス定義*」リストに表示されます。

定義を編集または削除するには、対応するボタンをクリックします。

注 – 定義タイプは後で変更できません。定義タイプを変更するには、サービス定義を削除し、希望の設定で新しいサービス定義を作成します。

5.3 時間帯定義

「*定義とユーザ > 時間帯定義*」ページで、単独または繰り返し発生する時間帯（タイムスロット）を定義できます。これを使用して、たとえばファイアウォールルールやコンテンツフィルタプロファイルの割り当てなどを特定の時間範囲に制限できます。

ヒント – 「*時間帯定義*」リストの時間帯定義の情報アイコンをクリックすると、その時間帯定義が使用されているすべての設定オプションを表示できます。

時間帯定義を作成するには、次の手順に従います。

1. **「*時間帯定義*」タブで、「*新規時間帯定義*」をクリックします。**
   「*新規時間帯定義の作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前: この時間帯定義を説明する名前を入力します。

   タイプ: 時間帯定義のタイプを選択します。次のタイプを使用できます。

   - **繰り返しイベント:** これらのイベントは定期的に繰り返されます。開始時間、終了時間、および時間帯定義が適用される曜日を選択できます。終了時間が翌日になる場合は、開始時間の曜日を選択します。このタイプには開始日と終了日は選択できません。
   - **単独イベント:** これらのイベントは一度だけ実施されます。開始日時および終了日時の両方を選択できます。これらの定義は繰り返されないので、「*曜日*」オプションはこのタイプには選択できません。
   - **コメント**（任意）: 説明などの情報を追加します。
3. **「*保存*」をクリックします。**
   新しい時間帯定義が「*時間帯定義*」リストに表示されます。

時間帯定義を編集あるいは削除するには、該当するボタンをクリックします。

5.4 ユーザとグループ

「*定義とユーザ*>*ユーザとグループ*」メニューを使用して、WebAdmin アクセス、リモートアクセス、ユーザポータルアクセス、メールの使用のためのユーザとグループを作成することができます。

5.4.1 ユーザ

「*定義とユーザ*>*ユーザとグループ*>*ユーザ*」タブで、UTMにユーザアカウントを追加することができます。Sophos UTMには、工場出荷時のデフォルト設定として、*admin*という1人の管理者が構成されています。

ヒント–「ユーザ」リストのユーザ定義の情報アイコンをクリックすると、ユーザ定義が使用されているすべての設定オプションを表示できます。

「*新規ユーザ*」ダイアログボックスでメールアドレスを指定すると、このユーザの X.509 証明書が生成されるのと同時に、メールアドレスを証明書の VPN ID として使用してユーザ定義が作成されます。メールアドレスが指定されていない場合は、ユーザの*識別名*(DN)を VPN ID として証明書が作成されます。このように、ユーザが eDirectory などのバックエンドグループにより認証されている場合は、対応するバックエンドユーザオブジェクトでメールアドレスが設定されていない場合でも証明書は作成されます。

なぜなら、各証明書の VPN ID は一意であるため、各ユーザ定義は異なる一意のメールアドレスを使用しているからです。システムにすでにあるメールアドレスを使用したユーザ定義の作成は失敗します。証明書は、Sophos UTMがサポートする各種リモートアクセス方法で使用可能です。ただし、PSK を使用する PPTP、L2TP over IPsec、および RSA または PSK を使用するネイティブ IPsec は除外されます。

ユーザアカウントを追加するには、以下の手順に従います。

1. **「ユーザ」タブで、「*新規ユーザ*」をクリックします。**
   「*新規ユーザの作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**

ユーザ名:このユーザを説明する名前を入力します(例: jdoe)。PPTP または L2TP over IPsec 経由のリモートアクセスを使用する場合、ユーザ名には印刷可能な ASCII 文字しか使用できないことがあります[1]。

実際の名前:ユーザの実際の名前を入力します(例: John Doe)。

メールアドレス:ユーザのプライマリメールアドレスを入力します。

他のメールアドレス(オプション):このユーザの他のメールアドレスを入力します。これらのメールアドレスに送信されたスパムメールは各メールアドレス用の個々の隔離レポートにリストされ、このレポートは前述のプライマリメールアドレスに送信されます。

認証:認証方式を選択します。以下の方式を使用できます。

- **ローカル:**UTMでユーザをローカル認証する場合に選択します。
- **リモート:**Sophos UTMでサポートされている外部認証方式のいずれかを使用してユーザを認証する場合に選択します。詳細は、「*定義とユーザ > 認証サーバ*」を参照してください。
- **なし:**ユーザが認証されるのを完全に防止する場合に選択します。これは、たとえば、ユーザ定義を削除することなくユーザを一時的に無効にする場合に役に立ちます。

パスワード:ユーザのパスワードを入力します(確認のために 2回入力します)。認証方式として「*ローカル*」を選択した場合のみ利用できます。基本的なユーザ認証ではウムラウトはサポートしていません。PPTP または L2TP over IPsec 経由のリモートアクセスを使用する場合、パスワードには印刷可能な ASCII 文字しか使用できないことがあります[2]。

バックエンド同期:実際の名前やユーザのメールアドレスなどのユーザ定義の基本設定の一部を、データを外部バックエンド認証サーバと同期することで自動的に更新できます(認証方式として「*リモート*」を選択したときのみ利用できます)。ユーザに対してプリフェッチが指定されている場合、このオプションは、「*認証サーバ > 詳細*」タブにある「*ログイン時のバックエンド同期を有効化*」オプションに従って自動的に設定されることに注意してください。

注 – 現在は、Active Directory および eDirectory サーバのデータのみ同期できます。

X.509 証明書:ユーザ定義を作成したら、ユーザ定義を編集する際にこのユーザに X.509 証明書を割り当てることができます。デフォルトでは、この証明書はユーザ定義を作成したと

[1] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters
[2] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters

きに自動的に生成されたものです。ただし、サードパーティの証明書を割り当てることもできます。証明書は、*「リモートアクセス」>「証明書管理」>「証明書」*タブでアップロードできます。../s2s/Certificate_Management-Certificates.htm

スタティックリモートアクセス IP を使用（オプション）:リモートアクセスを取得するユーザに、IP アドレスプールのダイナミック IP アドレスを割り当てる代わりにスタティック IP アドレスを割り当てる場合に選択します。NAT ルータ背後の IPsec ユーザは、スタティックリモートアクセス IP アドレスを必ず使用する必要があります。

注 – スタティックリモートアクセス IP は、PPTP、L2TP、および IPsec を介したリモートアクセスのみに使用できます。これは、SSL を介したリモートアクセスには使用できません。

コメント（任意）:説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   ユーザは独自のメールホワイトリストとブラックリストを作成し、管理することができます（「ユーザポータル」の章を参照）。ここでこれらのリストを参照し、必要に応じて変更することができます。
4. **「*保存*」をクリックします。**
   新しいユーザアカウントが「ユーザ」リストに表示されます。

このユーザを Web ベースの管理インタフェース WebAdmin へのアクセスをもつ正規の管理者にする場合は、そのユーザを *SuperAdmins* グループに追加します。SuperAdmins は、WebAdmin の「*定義とユーザ > ユーザとグループ > グループ*」タブで設定します。

注 – ユーザオブジェクトを削除した後で同じ名前でユーザオブジェクトを作成する場合は、このユーザに関連する証明書も*「リモートアクセス」>「証明書管理」>「証明書」*タブで削除したことを確認してください。削除していない場合、「その名前のアイテムはすでに存在します」という旨のエラーメッセージが表示されます。

何らかのリモートアクセスが有効化されたユーザのリモートアクセス証明書や設定をダウンロードすることができます。このためには、各ユーザの前にあるチェックボックスにチェックを入れ、リストヘッダの「アクション」ドロップダウンリストから目的のオプションを選択します。ユーザポータルの使用が許可されている場合は、リモートアクセスユーザ自身もこれらのファイルをダウンロードできます。

5.4.2 グループ

「*定義とユーザ*>*ユーザとグループ*>*グループ*」ページで、UTMにユーザグループを追加することができます。Sophos UTMには、工場出荷時のデフォルト設定として、*SuperAdmins* というユーザグループがあります。管理特権をユーザに割り当てたい（つまりWebAdminへのアクセス権をユーザに付与したい）場合は、当該ユーザを *SuperAdmins* グループに追加します。このグループは削除しないでください。

ヒント－「*グループ*」リストでグループの定義をクリックすると、そのグループ定義が使用されているすべての設定オプションが表示されます。

ユーザグループを追加するには、次の手順に従ってください。

1. **「*グループ*」タブで、「*新規グループ*」をクリックします。**
   「*新規グループの作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   グループ名:このグループを説明する名前を入力します。この名前は、バックエンドグループの名前に対応している必要はありません。

   グループタイプ:グループのタイプを選択します。スタティックメンバのグループか、ダイナミックメンバシップを実現する2種類のグループタイプから選択できます。

   - **スタティックメンバー:**このグループのメンバーとなるローカルユーザを選択します。
   - **IPsec X509 DN マスク:**ユーザは、IPsec 接続によってゲートウェイへのログインに成功し、識別名に含まれる特定のパラメータが「*DN マスク*」ボックスで指定された値と一致した場合に、IPsec X509 DN グループ定義に動的に追加されます。
   - **バックエンドメンバーシップ:**ユーザは、サポートされるいずれかの認証メカニズムによる認証が成功した場合に、グループ定義に動的に追加されます。続行するには、該当するバックエンド認証タイプを選択します。
     - **Active Directory:**UTMの Active Directory ユーザグループは、Windows ネットワーク上で設定されている Active Directory サーバユーザグループのメンバーに対し、グループメンバーシップを提供します。このユーザがメンバとなっている Active Directory サーバグループの名前を入力してください。詳細は、「*定義とユーザ*>*認証サーバ*>*サーバ*」を参照してください。
     - **eDirectory:**UTMの eDirectory ユーザグループは、eDirectory ネットワーク上で設定されている eDirectory ユーザグループのメンバーに対し、グループメン

バーシップを提供します。このユーザがメンバとなっている eDirectory グループの名前を入力してください。詳細は、「*定義とユーザ > 認証サーバ > サーバ*」を参照してください。

- **RADIUS:**ユーザは、RADIUS 認証方式による認証が成功すると、RADIUS バックエンドグループに自動的に追加されます。
- **TACACS+:**ユーザは、TACACS+ 認証方式による認証が成功すると、TACACS+ バックエンドグループに自動的に追加されます。
- **LDAP:**ユーザは、LDAP 認証方式による認証が成功すると、LDAP バックエンドグループに自動的に追加されます。

バックエンドグループメンバーシップに制限（オプション）:選択したバックエンドサーバのすべてのユーザをこのグループ定義に含めることを望まない場合は、すべての X.500 ベースのディレクトリサービスに対して、バックエンドサーバ上のいくつかのグループにメンバーシップを制限することができます。このオプションを選択する場合、ここで入力するグループは、バックエンドサーバに設定されている*一般名*と一致している必要があります。Active Directory バックエンドに対してこのオプションを選択する場合、`CN=` プレフィックスは省略できます。eDirectory バックエンドに対してこのオプションを選択すると、eDirectory ブラウザを使用して、このグループ定義に含める eDirectory グループを簡単に選択することができます。ただし、eDirectory ブラウザを使用しない場合は、eDirectory コンテナの入力時に `CN=` プレフィックスを必ず含めてください。

LDAP 属性のチェック（オプション）:選択したバックエンド LDAP サーバのすべてのユーザをこのグループ定義に含めたくはない場合は、このチェックボックスにチェックを入れて、バックエンドサーバ上にある特定の LDAP 属性に一致するユーザのみにメンバーシップを制限することができます。この属性は LDAP 検索フィルタとして使用されます。たとえば、属性として `groupMembership` を入力し、その値として `CN=Sales,O=Example` を入力することにより、これにより、会社の営業部門に属するすべてのユーザをグループ定義に含めることができます。

コメント（任意）:説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しいユーザグループが「*グループ*」リストに表示されます。

グループを編集または削除するには、対応するボタンをクリックします。

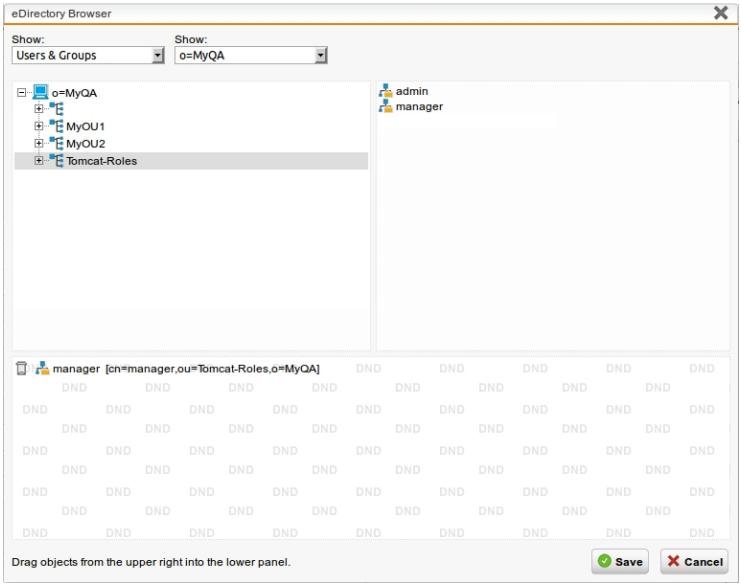

Figure 17 グループ: Sophos UTM

5.5 クライアント認証

Sophos は、UTMで直接ユーザ認証を行うために、Windows 用の認証クライアントを提供しています。これにより、ユーザネットワークまたはグループネットワークに基づくファイアウォールルールを作成したりすることで、Web サーフィンやネットワークトラフィックをユーザに基づいてコントロールすることができます。さらに、可能であれば、IP アドレス、ホスト名、その他の情報をユーザ名に置き換えるため、データやオブジェクトのレポートがより読みやすくなります。

注 – WebAdmin では、クライアント認証で認証されたユーザオブジェクトは、パフォーマンス上の理由から常に未解決として表示されます。

クライアント認証を使用したい(あるいは使用する必要がある)ユーザは、クライアント PC または Mac OS コンピュータに Sophos Authentication Agent (SAA)をインストールする必要があります。SAA は、この WebAdmin ページまたはユーザポータルからダウンロード可能です。ユーザポータルのページにダウンロードリンクが表示されるのは、クライアント認証設定のユーザグループに参加しているユーザのみです。

クライアント認証を設定するには、次の手順に従ってください。

1. **「*クライアント認証*」タブで、クライアント認証を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、「*クライアント認証オプション*」エリアが編集可能になります。

2. **許可するネットワークを選択します。**
   クライアント認証を使用する必要があるネットワークを選択します。クライアント認証が機能するためには、これらのネットワークがUTMに直接接続されている必要があります。

3. **許可するユーザおよびグループを選択します。**
   単一のユーザおよびグループを「*許可されるユーザおよびグループ*」ボックスで選択または追加します。これは、既存の認証グループ（Active Directory ユーザグループなど）にすることもできます。

4. **「*適用*」をクリックします。**
   設定が保存されます。

   選択したネットワークでクライアント認証を利用できるようになりました。

クライアント認証プログラム

クライアント認証を有効にすると、ここで Sophos Authentication Agent（SAA）をダウンロードできます。SAA を手動で配布するか、ユーザがユーザポータルからダウンロードできるようにすることができます。

EXE ファイルのダウンロード:クライアント PC に直接インストールするための CA 証明書を含むクライアント認証プログラムをダウンロードします。これは、ユーザポータルからダウンロードできるものと同じファイルです。

MSI ファイルのダウンロード:クライアント認証 MSI パッケージをダウンロードします。このパッケージはドメインコントローラ（DC）を通じて自動でパッケージをインストールするためのもので、ここには CA 証明書は含まれません。

DMG のダウンロード:クライアント認証 Mac OS X ディスクイメージをダウンロードします。このイメージは OS X を稼働しているクライアント PC にインストールする場合に使用します。

CA のダウンロード:MSI パッケージに追加して CA 証明書をインストールする必要がある場合にダウンロードします。

SAAは Web フィルタの認証モードとして使用できます。詳しくは、「*Web プロテクション > Web フィルタリング > グローバル*」の章を参照してください。

5.6 認証サーバ

「*定義とユーザ > 認証サーバ*」ページでは、外部ユーザ認証サービスのデータベースおよびバックエンドサーバを管理できます。外部ユーザ認証を使用すると、ネットワーク内の他のサーバ上にある既存のユーザデータベースやディレクトリサービスに対して、ユーザアカウントを検証することができます。現在サポートされている認証サービスは次のとおりです。

- Novell の eDirectory
- マイクロソフトの Active Directory
- RADIUS
- TACACS+
- LDAP

5.6.1 グローバル設定

「*定義とユーザ > 認証サーバ > グローバル設定*」タブを使用すると、基本的な認証オプションを設定できます。次のオプションを使用できます。

自動的にユーザを作成:このオプションを選択した場合、設定済みのバックエンドグループの不明ユーザが、Sophos UTM でサポートされている各種認証サービスのいずれかに対する認証に成功すると、Sophos UTM は常にユーザオブジェクトを自動作成します。例えば、RADIUS バックエンドグループを設定しており、「*マネジメント*」>「*WebAdmin 設定*」>「*アクセスコントロール*」タブで定義したいずれかのロールにこのグループをメンバーとして追加する場合、Sophos UTM は WebAdmin へのログインに成功した RADIUS ユーザに対してユーザ定義を自動的に作成します。

- **機能別自動ユーザ作成:**自動ユーザ作成は、特定のサービスに対して有効または無効にすることができます。有効なサービスに対してのみ、ユーザが作成されます。「*自動的にユーザを作成*」オプションからチェックを外すと、このオプションは使用できず、ユーザの自動作成機能はすべての機能に対して無効になります。

  注 – この機能は、Active Directory の *シングルサインオン*(SSO)では機能しません。

これらのユーザオブジェクトは、Sophos UTMのユーザポータル へのアクセス権を付与するためにも必要になります。さらに、自動作成されたすべてのユーザオブジェクトのために、X.509 証明書が生成されます。ただし、メールアドレスがすでに存在するアドレスと衝突する場合は、このユーザの自動作成は失敗します。この理由は、自動的に作成されるユーザ定義において、システムにすで

に存在するメールアドレスを設定すべきではないためです。メールアドレスは X.509 証明書の識別子として使用されるため、すべてのメールアドレスはシステム内で一意でなければなりません。

重要 – ユーザオブジェクトが自動作成されたユーザに対する認証（ユーザが何者であるかを判断するためのアクション）と権限付与（ユーザが何を許可されているかを判断するためのアクション）は、常にリモートのバックエンドサーバ/ディレクトリサービス上で実行されます。そのため、対応するバックエンドサーバが使用不能な場合や、そのリモートサイトでユーザオブジェクトが削除されている場合には、Sophos UTMで自動的に作成されたユーザオブジェクトは機能しません。

また、Active Directory の *シングルサインオン*（SSO）を除き、Sophos UTMはリモート認証サーバから取得したユーザ認証データを 300秒間キャッシュします。このため、リモートユーザ設定への変更は、キャッシュの期限が切れた後で初めて有効になります。

認証キャッシュ

Sophos UTMが不明ユーザから `http` などのユーザ要求を受信し、認証が必要である場合は、SophosUser Authentication（SUA）が必ず認証キャッシュにエントリを書き込みます。長期的に、ユーザが頻繁に変わるような環境では、適宜キャッシュを空にすることが合理的です。また、すべてのユーザに対して、新たな認証を今すぐ強制したい場合には、「*認証キャッシュをクリア*」ボタンを使用して、認証キャッシュを空にしてください。
認証は 300秒間有効です。この間、同じユーザから他の認証要求があったときには、直接キャッシュが検索されます。この方法により、eDirectory などのバックエンド認証サービスにかかる負荷を軽減できます。

注 – キャッシュのクリアは、リモートログイン中のユーザには影響がありません。

ライブログ

ライブログを開く:このボタンをクリックすると、新しいウィンドウに *User Authentication*（SUA）のログが表示されます。

5.6.2 サーバ

「*定義とユーザ > 認証サーバ > サーバ*」タブで、1つ以上の認証サーバ（eDirectory、Active Directory、LDAP、RADIUS、TACACS+など）を作成できます。

5.6.2.1 eDirectory

Novell eDirectory は、あるネットワーク内の複数のサーバとコンピュータ上にあるリソースへのアクセスを一元管理するための X.500 互換ディレクトリサービスです。eDirectory は階層構造のオブジェクト指向データベースであり、組織内のすべての資産を論理ツリーで表現します。資産には、人、サーバ、ワークステーション、アプリケーション、プリンタ、サービス、グループなどが含まれます。

eDirectory 認証を設定するには、次の手順に従ってください。

1. **「*サーバ*」タブで、「*新規認証サーバ*」をクリックします。**
   「*新規認証サーバ*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   バックエンド:バックエンドのディレクトリサービスとして「*eDirectory*」を選択します。

   位置:バックエンドサーバの位置を選択します。番号が小さいバックエンドサーバから順に問い合わせが行われます。パフォーマンスを向上するためには、要求を最も多く受けると予想されるバックエンドサーバをリストの一番上に配置します。

   サーバ:eDirectory サーバを選択(または追加)します。

   SSL:SSL データ転送を有効にするには、このオプションを選択します。すると、*ポート*が 389 (LDAP)から 636 (ldaps = LDAP over SSL)に変わります。

   ポート:eDirectory サーバのポートを入力します。デフォルトで、ポート 389 が選択されています。

   Bind DN:サーバにバインドするユーザの*識別名*(DN)を指定します。eDirectory サーバへの匿名での問い合わせが許可されていない場合、このユーザが必要です。バインドユーザには、関連するすべてのユーザオブジェクト情報を eDirectory サーバから取得してユーザの認証を行うために必要な特権が付与されている必要があります。eDirectory ユーザ、グループ、コンテナは、LDAP 表記法で完全識別名として指定します。区切り文字にはコンマを使用します(例: `CN=administrator,DC=intranet,DC=example,DC=com`)。

   パスワード:バインドユーザのパスワードを入力します。

   サーバ設定のテスト:「テスト」ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバが起動しており、接続を受け付けていることが確認されます。

Base DN:LDAP ツリーのルートに相対的な開始位置で、ここに認証されるユーザが含まれています。ベース DN は、LDAP 表記の完全識別名 (FDN) で、コンマを区切り文字として使用して指定する必要があります (例: `O=Example,OU=RnD`)。ベース DN は空にすることもできます。この場合は、ベース DN は自動的にディレクトリから取り出されます。

ユーザ名:認証を実行するテストユーザのユーザ名を入力してください。

パスワード:テストユーザのパスワードを入力します。

テストユーザで認証を行う:「テスト」ボタンをクリックして、テストユーザの認証テストを開始します。これにより、すべてのサーバ設定が正しいこと、サーバが稼働中で接続を受け付けていること、およびユーザを正常に認証できることを確認できます。

3. **「*保存*」をクリックします。**
   サーバが「*サーバ*」リストに表示されます。

5.6.2.2 Active Directory

Active Directory (AD) とは、マイクロソフトが実装したディレクトリサービスであり、Windows 2000/2003 Server の中核を成すコンポーネントです。Active Directory には、ユーザ、グループ、コンピュータ、プリンタ、アプリケーション、サービス、あらゆる種類のユーザ定義オブジェクトなど、ネットワーク内に存在するさまざまなリソースに関する情報が保存されます。このため、Active Directory には、これらのリソースへのアクセスを一元的に体系化し、管理し、コントロールするための機能が用意されています。

Active Directory 認証方式では、Sophos UTMをWindowsドメインに登録し、プライマリの*ドメインコントローラ*(DC) にSophos UTM用のオブジェクトを作成します。UTMこれにより、UTM は、このドメインのユーザとグループに関する情報を問い合わせることが可能になります。

注 – UTM は Active Directory 2003 以降に対応しています。

Active Directory 認証を設定するには、次の手順に従ってください。

1. **「*サーバ*」タブで、「*新規認証サーバ*」をクリックします。**
   「*新規認証サーバの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   バックエンド:バックエンドのディレクトリサービスとして「*Active Directory*」を選択します。

位置:バックエンドサーバの位置を選択します。番号が小さいバックエンドサーバから順に問い合わせが行われます。パフォーマンスを向上するためには、要求を最も多く受けると予想されるバックエンドサーバをリストの一番上に配置します。

サーバ: Active Directory サーバを選択(または追加)します。

SSL:SSL データ転送を有効にするには、このオプションを選択します。すると、*ポート*が 389 (LDAP)から 636 (ldaps = LDAP over SSL)に変わります。

ポート: Active Directory サーバのポートを入力します。デフォルトで、ポート 389 が選択されています。

Bind DN:サーバにバインドするユーザの完全な*識別名*(DN)を LDAP 表記法で指定します。eDirectory サーバへの匿名での問い合わせが許可されていない場合、このユーザが必要です。バインドユーザには、関連するすべてのユーザオブジェクト情報を Active Directory サーバから取得してユーザの認証を行うために必要な特権を付与する必要があります。通常は、ドメインの管理者がこの要件に対応します。

各 DN は、Active Directory ユーザオブジェクトのいくつかの属性から成る 1つ以上の RDN (*相対識別名*)で構成されます。ユーザ名、常駐するノード、サーバのトップレベル DNなどを、コンマ区切りの LDAP 表記法で記述します。

- ユーザ名は、ディレクトリにアクセスできるユーザの名前にする必要があり、CN 識別子(CN=userなど)で指定します。ドメイン権限を持つ「admin」などの一般的なアカウントを使用することもできますが、ベストプラクティスとしては、admin 権限を持たないユーザを指定することが推奨されます。この理由は、所与のベース DN を起点とするサブツリー内の全オブジェクトに対する読み取り権限さえあれば十分であるためです。
- ユーザオブジェクトが保存されているノードの情報には、ルートノードからユーザオブジェクトまですべてのサブノードが含まれている必要があり、通常はいわゆる*組織ユニット*コンポーネントや*一般名*コンポーネントから構成されます。組織ユニット(Microsoft Management Console では、フォルダと本を組み合わせたアイコンで示される)は、識別子 OU を使用して指定します。ノードは、最も低いノードから順に並べられ、末尾は最も高いノードになります。つまり、先頭は最も詳細な要素になります(例: OU=Management_US,OU=Management)。一方、事前定義されている *Users* ノードなどのデフォルト Active Directory コンテナ(シンプルなフォルダアイコンで示される)は、識別子 CN で指定します(例: CN=Users)。
- サーバのトップレベル DN は、それぞれ識別子 DC で指定されている複数のドメインコンポーネントから構成することができます。ドメインコンポーネントはドメイン名と同じ

順序で指定します(たとえば、ドメイン名がexample.comである場合、DN部分はDC=example,DC=comとします)。

たとえば、名前が administrator であり、オブジェクトが example.comドメインの Users コンテナに保存されるバインドユーザのDNは次のようになります。CN=administrator,CN=Users,DC=example,DC=com

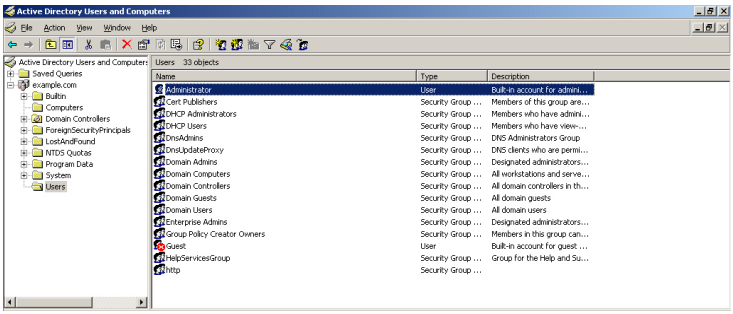

Figure 18 認証:Microsoft Management Console

ここで、*Management* という名前の組織ユニットを作成し、サブノードを *Management_US* とし、管理者ユーザオブジェクトをこのサブノードに移動すると、管理者の DN は次のように変わります。CN=administrator,OU=Management_US,OU=Management,DC=example,DC=com

パスワード:バインドユーザのパスワードを入力します。

サーバ設定のテスト:「*テスト*」ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバが起動しており、接続を受け付けていることが確認されます。

Base DN:LDAP ツリーのルートに相対的な開始位置で、ここに認証されるユーザが含まれています。ベース DN は、LDAP 表記の完全識別名 (FDN) で、コンマを区切り文字として使用して指定する必要があります(例: O=Example,OU=RnD)。ベース DN は空にすることもできます。この場合は、ベース DN は自動的にディレクトリから取り出されます。

ユーザ名:認証を実行するテストユーザのユーザ名を入力してください。

パスワード:テストユーザのパスワードを入力します。

テストユーザで認証を行う:「*テスト*」ボタンをクリックして、テストユーザの認証テストを開始します。これにより、すべてのサーバ設定が正しいこと、サーバが稼働中で接続を受け付けていること、およびユーザを正常に認証できることを確認できます。

3. **「*保存*」をクリックします。**
   サーバが「サーバ」リストに表示されます。

5.6.2.3 LDAP

LDAP とは、「*Lightweight Directory Access Protocol*」の略であり、X.500 標準に基づいてディレクトリサービスの問い合わせと変更を行うネットワーキングプロトコルです。Sophos UTMでは、複数のサービスへのユーザ認証に LDAP プロトコルを使用しており、LDAP サーバに設定された属性やグループメンバシップに基づいてアクセスを許可または却下します。

LDAP 認証を設定するには、次の手順に従ってください。

1. **「*サーバ*」タブで、「*新規認証サーバ*」をクリックします。**
   「*新規認証サーバの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   バックエンド:バックエンドのディレクトリサービスとして「*LDAP*」を選択します。

   位置:バックエンドサーバの位置を選択します。番号が小さいバックエンドサーバから順に問い合わせが行われます。パフォーマンスを向上するためには、要求を最も多く受けると予想されるバックエンドサーバをリストの一番上に配置します。

   サーバ:LDAP サーバを選択(または追加)します。

   SSL:SSL データ転送を有効にするには、このオプションを選択します。すると、*ポート*が `389`(LDAP)から `636`(ldaps = LDAP over SSL)に変わります。

   ポート:LDAP サーバのポートを入力します。デフォルトで、ポート `389` が選択されています。

   Bind DN:サーバにバインドするユーザの*識別名*(DN)を指定します。このユーザは必須です。セキュリティ上の理由から、LDAP サーバへの匿名での問い合わせはサポートされていません。バインドユーザには、関連するすべてのユーザオブジェクト情報を LDAP サーバから取得してユーザを認証するために必要な特権が付与されている必要があります。LDAPユーザ、グループ、コンテナは、LDAP 表記法で完全識別名として指定します。区切り文字にはコンマを使用します。(例:
   `CN=administrator,DC=intranet,DC=example,DC=com`)

   パスワード:バインドユーザのパスワードを入力します。

   サーバ設定のテスト:「テスト」ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバが起動しており、接続を受け付けていることが確認されます。

ユーザ属性:LDAP ディレクトリ検索用のフィルタとして使用されるユーザ属性を選択します。ユーザ属性には、リモートアクセスサービスなどが各ユーザに対してプロンプト表示する実際のログイン名が含まれます。次のユーザ属性を選択できます。

- CN(一般名)
- SN(姓)
- UID(ユーザ ID)

LDAP ディレクトリのユーザ名がこれらのフォームに保存されていない場合、リストで*カスタム(<<Custom>>)*を選択し、下の「*カスタム*」フィールドにカスタム属性を入力します。この属性は LDAP ディレクトリで設定する必要があります。

Base DN:LDAP ツリーのルートに相対的な開始位置で、ここに認証されるユーザが含まれています。ベース DN は、LDAP 表記の完全識別名(FDN)で、コンマを区切り文字として使用して指定する必要があります(例: `O=Example,OU=RnD`)。ベース DN は空にすることもできます。この場合は、ベース DN は自動的にディレクトリから取り出されます。

ユーザ名:認証を実行するテストユーザのユーザ名を入力してください。

パスワード:テストユーザのパスワードを入力します。

テストユーザで認証を行う:「*テスト*」ボタンをクリックして、テストユーザの認証テストを開始します。これにより、すべてのサーバ設定が正しいこと、サーバが稼働中で接続を受け付けていること、およびユーザを正常に認証できることを確認できます。

3. **「*保存*」をクリックします。**
   サーバが「*サーバ*」リストに表示されます。

5.6.2.4 RADIUS

RADIUSとは、「*Remote Authentication Dial In User Service*」の略であり、ルータなどのネットワークデバイスで中央データベースに対してユーザを認証するために広く用いられているプロトコルです。RADIUS には、ユーザの情報に加え、ネットワークデバイスで使用される技術情報(サポートされるプロトコル、IP アドレス、ルーティング情報など)も保存できます。この情報は、RADIUS サーバ上のファイルまたはデータベースに保存されるユーザプロファイルを構成します。

RADIUS プロトコルは非常に柔軟であり、サーバはほとんどのオペレーティングシステムで利用可能です。UTMに RADIUS を導入することで、プロキシとユーザに基づいてアクセス権限を設定できるようになります。RADIUS 認証を使用するためには、ネットワーク上で稼働している RADIUS サーバが必要です。パスワードは平文(暗号化なし)で送信されるため、UTMと同じネットワーク内に RADIUS サーバを配置してください。また、UTMとサーバは同じスイッチに接続してください。

RADIUS 認証を設定するには、次の手順に従ってください。

1. **「サーバ」タブで、「*新規認証サーバ*」をクリックします。**
   「*新規認証サーバの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   バックエンド:バックエンドのディレクトリサービスとして「*RADIUS*」を選択します。

   位置:バックエンドサーバの位置を選択します。番号が小さいバックエンドサーバから順に問い合わせが行われます。パフォーマンスを向上するためには、要求を最も多く受けると予想されるバックエンドサーバをリストの一番上に配置します。

   サーバ:RADIUS サーバを選択(または追加)します。

   ポート:RADIUS サーバのポートを入力します。デフォルトで、ポート `1812` が選択されています。

   共有シークレット:共有シークレットとは、RADIUS クライアントと RADIUS サーバの間でパスワードとしての役割を果たすテキスト文字列です。共有シークレットを入力します。

   サーバ設定のテスト:「*テスト*」ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバが起動しており、接続を受け付けていることが確認されます。

   ユーザ名:認証を実行するテストユーザのユーザ名を入力してください。

   パスワード:テストユーザのパスワードを入力します。

   NAS 識別子:適切な NAS 識別子をリストから選択します。詳細は、注記と下の表を参照してください。

   テストユーザで認証を行う:「*テスト*」ボタンをクリックして、テストユーザの認証テストを開始します。これにより、すべてのサーバ設定が正しいこと、サーバが稼働中で接続を受け付けていること、およびユーザを正常に認証できることを確認できます。

3. **「*保存*」をクリックします。**
   サーバが「*サーバ*」リストに表示されます。

注 – RADIUS サーバに問い合わせを行う、Sophos UTM の各ユーザ認証サービス(PPTP や L2TP など)は、異なる識別子(NAS 識別子)を RADIUS サーバに送信します。たとえば、PPTP サービスは、このユーザの認証を試みるときに、`pptp` という NAS 識別子を RADIUS サーバに送信します。これにより、RADIUS サーバがさまざまなサービスを識別して特定の種類のサービスをユーザに付与することができるため、権限付与の目的で役に立ちます。ユーザ認証サービスとそれに対応する NAS 識別子のリストは以下のとおりです。

ユーザ認証サービス	NAS 識別子
SSL VPN	ssl
PPTP	pptp
IPsec	ipsec
L2TP over IPsec	l2tp
SMTPプロキシ	smtp
ユーザポータル	portal
WebAdmin	webadmin
SOCKS プロキシ	socks
Web フィルタ	http
認証クライアント	エージェント
ワイヤレスアクセスポイント	NAS ID はワイヤレスネットワーク名です。

Table 1: RADIUS NAS 識別子

5.6.2.5 TACACS+

TACACS+(「*Terminal Access Controller Access Control System*」の略語)とは、Cisco Systems, Inc. 独自のプロトコルであり、認証プロセスと権限付与プロセスについて詳細なアカウンティング情報と管理的なコントロールを提供します。RADIUS では認証と権限付与がユーザプロファイルにまとめられていますが、TACACS+ ではこれらのオペレーションを区別しています。他の相違点としては、TACACS+ では TCP プロトコル(ポート 49)を使用し、RADIUS では UDP プロトコルを使用します。

TACACS+ 認証を設定するには、次の手順に従ってください。

1. **「サーバ」タブで、「*新規認証サーバ*」をクリックします。**
   「*新規認証サーバの作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   バックエンド:バックエンドのディレクトリサービスとして「*TACACS+*」を選択します。

位置:バックエンドサーバの位置を選択します。番号が小さいバックエンドサーバから順に問い合わせが行われます。パフォーマンスを向上するためには、要求を最も多く受けると予想されるバックエンドサーバをリストの一番上に配置します。

サーバ:TACACS+ サーバを選択(または追加)します。

ポート:TACACS+ サーバのポートを入力します。デフォルトで、ポート 49 が選択されています。

キー: Sophos UTM と TACACS+ サーバの間のすべての TACACS+ 通信に使用する認証および暗号鍵を入力します。ここで入力する鍵の値は、TACACS+ サーバで設定した値と一致している必要があります。鍵を入力してください(確認のために 2回)。

サーバ設定のテスト:「*テスト*」ボタンを押すと、設定されたサーバとのバインドテストが実行されます。これにより、このタブの設定が正しいこと、およびサーバが起動しており、接続を受け付けていることが確認されます。

ユーザ名:認証を実行するテストユーザのユーザ名を入力してください。

パスワード:テストユーザのパスワードを入力します。

テストユーザで認証を行う:「*テスト*」ボタンをクリックして、テストユーザの認証テストを開始します。これにより、すべてのサーバ設定が正しいこと、サーバが稼働中で接続を受け付けていること、およびユーザを正常に認証できることを確認できます。

3. **「*保存*」をクリックします。**
   サーバが「*サーバ*」リストに表示されます。

5.6.3 シングルサインオン

「*定義とユーザ*>*認証サーバ*>*シングルサインオン*」タブでは、Active Directory または eDirectory (あるいはその両方)のシングルサインオン機能を設定できます。

Active Directory のシングルサインオン(SSO)

Active Directoryの SSO 機能は現在、Web フィルタのみで使用されており、NTLMv2 または Kerberos 認証をサポートするブラウザでシングルサインオン機能を使用できます。

シングルサインオン機能を有効にするには、UTMをActive Directoryドメインに追加する必要があります。追加するドメインが機能するためには、次の前提条件を満たしている必要があります。

- ゲートウェイとドメインコントローラ(DC)のタイムゾーンが同じである。
- ゲートウェイのクロックとDC のクロックの間に、5分を超える時刻差がない。

- UTMホスト名が AD DNS システムに存在する。
- UTM が AD DNS をフォワーダとして使用しているか、AD ドメインに対して AD DNS サーバをターゲットとする DNS リクエストルートが定義されている。

Active Directory SSO を設定するには、次の手順に従ってください。

1. **Active Directory サーバを「*サーバ*」タブで作成します。**
2. **次の設定を行います。**
   ドメイン:ドメインの名前（`intranet.mycompany.com` など）。UTMは DNS を使用して取得可能なすべての DC を検索します。

   アドミンユーザ名:管理者権限があり、ドメインにコンピュータを追加することが許可されているユーザ（通常は「管理者」）。

   パスワード:アドミンユーザのパスワード。
3. **「*適用*」をクリックします。**
   設定が保存されます。

Kerberos 認証サポートに関する注記:SSO Kerberos サポートが機能するためには、クライアントはプロキシ設定でUTMの FQDN ホスト名を使用する必要があります。IP アドレスを使用すると機能しません。NTLMv2 モードは、この要件の影響を受けません。この要件が満たされていない場合や、ブラウザが Kerberos 認証をサポートしない場合には、NTLMv2 モードが自動的に使用されます。

eDirectory のシングルサインオン（SSO）

ここでは、eDirectory 用に SSO を設定できます。「*Web プロテクション > Web フィルタリング*」で認証方式として *eDirectory SSO* を設定した場合、ここで選択した eDirectory サーバが使用されます。

eDirectory SSO を設定するには、次の手順に従ってください。

1. **eDirectory サーバを「*サーバ*」タブに登録します。**
2. **次の設定を行います。**
   サーバ: SSO を有効にする eDirectory サーバ。

   同期間隔:UTM と eDirectory サーバ間での同期イベントの間隔（秒数）。
3. **「*適用*」をクリックします。**
   設定が保存されます。

5.6.4 詳細

パスワード推測のブロック

この機能を使用してパスワードが推測されないようにします。設定した回数のログインに失敗すると(デフォルトでは 3回)、任意の機能へアクセスしようとしているIP アドレスは設定した時間(デフォルトでは 600秒間)ブロックされます。

ブロックされたホストからのパケットをドロップ:このオプションが有効になっていると、ブロックされたホストからのすべてのパケットは設定した時間内はドロップされます。このオプションにより、DoS 攻撃を回避できます。

機能:選択した機能のチェックが行われます。

ブロック対象外ネットワーク:ボックスにリストされているネットワークは、このチェックから除外されます。

ローカル認証パスワード

このオプションを使用すると、管理者や管理者権限を持つローカル登録ユーザに対して、パスワードの強化を強制することができます。次のセキュリティ要件を遵守するパスワードの複雑性を設定できます。

- 最小パスワード長。デフォルトは 8文字
- 小文字が 1つ以上必要
- 大文字が 1つ以上必要
- 数字が 1つ以上必要
- 英数字以外の文字が 1つ以上必要

選択したパスワードプロパティを有効にするためには、「*複雑なパスワードを必須にする*」チェックボックスにチェックを入れて、「*適用*」をクリックします。

ディレクトリユーザのプリフェッチ

eDirectory または Active Directory のユーザをUTMと同期することができます。これにより、UTMにユーザオブジェクトが事前に作成され、当該ユーザがログインしたときには、これらのユーザオブジェクトがすでに存在しています。同期プロセスは週次または日次で実行できます。

プリフェッチを有効にするには、次の設定を行います。

サーバ:ドロップダウンリストには、サーバタブで作成されたサーバが含まれています。プリフェッチを有効にするサーバを選択します。

プリフェッチ間隔:ユーザをプリフェッチする間隔を選択します。同期を週次で実行する場合、同期を開始する曜日を選択します。同期を日次で実行する場合、「*デイリー*」を選択します。

プリフェッチ時刻:ユーザをプリフェッチする時間を選択します。

グループ:どのグループを事前に作成するか指定するには、ここでグループを入力します。統合 LDAP ブラウザを使用して、これらのグループを選択できます。

ログイン時のバックエンド同期を有効化 (オプション):各プリフェッチイベントに対して、関連するユーザ (「*ユーザとグループ > ユーザ*」タブ) の「*バックエンド同期*」オプションは、ここで指定する値に設定されます。このオプションを有効にすると、ユーザの「*バックエンド同期*」オプションは有効化され、無効にすると、ユーザの「*バックエンド同期*」オプションは無効化されます。

設定を保存するには「*適用*」をクリックします。

直ちにプリフェッチ:プリフェッチを今すぐ開始するには、このボタンをクリックします。

プリフェッチライブログを開く:プリフェッチのライブログを開くには、このボタンをクリックします。

6 インタフェースとルーティング

この章では、Sophos UTM でインタフェースとネットワーク固有の設定を構成する方法について説明します。WebAdminの「*ネットワーク統計*」ページには、今日の上位 10件のアカウンティングサービス、上位送信元ホスト、および同時接続の概要が表示されます。各セクションには「*詳細*」リンクがあります。リンクをクリックするとWebAdmin の該当するレポートセクションが表示され、詳細な統計情報を参照できます。

この章では、次のトピックについて説明します。

- インタフェース
- ブリッジ
- QoS
- アップリンクモニタリング
- IPv6
- スタティックルーティング
- OSPF
- BGP
- マルチキャストルーティング (PIM-SM)

6.1 インタフェース

ゲートウェイには、内部 LAN を外部ネットワーク (インターネットなど) にセキュリティを維持して接続するために、少なくとも 2つのネットワークインタフェースカードが必要です。次の例では、ネットワークカード `eth0` は、常に、内部ネットワークに接続されるインタフェースです。一方、ネットワークカード `eth1` は、外部ネットワーク (インターネットなど) に接続されるインタフェースです。これらのインタフェースは、それぞれ信頼されるインタフェース、信頼されないインタフェースとも呼ばれます。

ネットワークカードは、インストール中に自動認識されます。ソフトウェアアプライアンスでは、新しいネットワークカードを後で追加すると、新たなインストールが必要になります。システムの再インストールを行うには、設定のバックアップを作成し、ソフトウェアをインストールし、バックアップを復元するだけです。

内部ネットワークと外部ネットワークの接点は、ゲートウェイのみであるようにしてください。すべてのデータは UTM を通過する必要があります。内部インタフェースと外部インタフェースを 1つのハブまたはスイッチに接続することは推奨しません。ただし、スイッチが、VLAN スイッチとして設定されている場合は除きます。誤った ARP（アドレス解決プロトコル）解決が発生する可能性があり、これを「ARP クラッシュ」と呼びます。この状況は、（マイクロソフト製品など）OS によっては管理できないものもあります。このため、各ゲートウェイネットワークインタフェースに対して、1つの物理ネットワークセグメントを使用する必要があります。

「*インタフェース*」メニューでは、UTM にインストールされているすべてのネットワークカードを設定・管理したり、外部ネットワーク（インターネット）へのすべてのインタフェースや内部ネットワーク（LAN、DMZ）へのインタフェースを設定・管理したりすることができます。

注 – ネットワークトポロジを計画し、UTM を設定しているときは、どのインタフェースがどのネットワークに接続しているかに注意してください。ほとんどの設定で、SysID が `eth1` のネットワークインタフェースが、外部ネットワークへの接続として選択されます。冗長化（HA）フェイルオーバーをインストールするためには、同じ SysID のネットワークカードを両システムで選択する必要があります。HA フェイルオーバーのインストールについて詳細は、*管理 > 冗長化*のページを参照してください。

次のセクションでは、「*インタフェース*」、「*追加アドレス*」、「*リンクアグリゲーション*」、「*アップリンクバランシング*」、「*マルチパスルール*」、「*ハードウェア*」のタブで、さまざまなインタフェースタイプを管理・設定する方法について説明します。

6.1.1 インタフェース

「*インタフェース*」タブでは、ネットワークカードと仮想インタフェースを設定できます。リストには、すでに定義されているインタフェースが、シンボル名、ハードウェアデバイス、現在のアドレスとともに表示されます。インタフェースのステータスも表示されます。トグルスイッチをクリックして、インタフェースを有効または無効に切り替えることができます。インタフェースグループにはトグルスイッチがないことに注意してください。

ヒント – 「*インタフェース*」リストにあるインタフェース定義の情報アイコンをクリックすると、該当するインタフェース定義を使用している設定オプションすべてを表示できます。

新規追加したインタフェースは、そのセットアップ中、「*無効*」と表示される場合があります。各インターフェースは、対応するボタンをクリックして、編集または削除することができます。

6.1.1.1 自動インタフェースネットワーク定義

UTM の各インタフェースには、シンボル名とハードウェアデバイスが割り当てられています。シンボル名は、他の構成設定でインタフェースを参照するときに使用します。各インタフェースについて、次のような対応するネットワーク定義のセットが UTM によって自動的に作成されます。

- インタフェースの現在の IP アドレス、およびインタフェース名と*(アドレス)*サフィックスから成る名前が含まれる定義。
- インタフェースに接続されたネットワーク、およびインタフェース名と*(ネットワーク)*サフィックスから成る名前が含まれる定義。この定義は、*PPP* タイプのインタフェースに対しては作成されません。
- インタフェースのブロードキャストアドレス、およびインタフェース名と*(ブロードキャスト)*サフィックスから成る名前が含まれる定義。この定義は、*PPP* タイプのインタフェースに対しては作成されません。

インタフェースで動的アドレス割り当て方法(DHCP やリモート割り当てなど)が使用されている場合、これらの定義は自動的に更新されます。ファイアウォールや NAT ルールなど、これらの定義を参照するすべての設定も、変更されたアドレスで自動的に更新されます。

「*Internal*」(内部)というシンボル名のインタフェース 1つが事前に定義されています。これは管理用インターフェースであり、通常、「内部」UTM インタフェースとして使用されます。この名前を変更するには、インストール直後に行う必要があります。

6.1.1.2 インタフェースタイプ

UTM に追加可能なインタフェースの種類と、それをサポートするために必要なハードウェアの種類は次のとおりです。

グループ:インタフェースをグループ化することができます。これにより、該当する構成では、複数のインタフェースを個別に選択する代わりに、1つのインタフェースグループを選択できるようになります。

3G/UMTS:これは、USB モデムスティック用のインタフェースです。インタフェースを作成する前に、モデムスティックを差し込み、UTM を再起動する必要があります。

DSL (PPPoA/PPTP):PPP over ATM。DSL PPPoA デバイスでは、ゲートウェイを *PPP-over-ATM* 互換の DSL 回線に接続できます。これらのデバイスは、PPTP プロトコルを使用して IP パケットをトンネリングします。これらのデバイスには専用イーサネット接続が必要です(同じハードウェア上で他のインタフェースと共存できません)。DSL モデムをインタフェースネットワークセグメントに接続する必要があります。これらのデバイスタイプのネットワークパラメータは、リモートステーション(使

用しているISP など）で割り当てることができます。さらに、ISP アカウントのユーザ名およびパスワードを入力する必要があります。また、使用しているモデムの IP アドレスも入力する必要があります。このアドレスは通常モデムに組み込まれているため変更できません。モデムで通信するには、NIC IP アドレスとネットマスクを入力する必要があります。モデムの IP アドレスは、これらのパラメータで定義されたネットワーク範囲内である必要があります。*Ping 先アドレス*は、ICMP ping 要求に応答するPPTP リンクの反対側のホストである必要があります。使用しているISP の DNS サーバを指定できます。このアドレスで ping できなかった場合、接続に問題があると判断され、再試行されます。

DSL (PPPoE):PPP over Ethernet。DSL PPPoE デバイスでは、ゲートウェイを *PPP-over-Ethernet* 互換の DSL 回線に接続できます。これらのデバイスには専用イーサネット接続が必要です（同じハードウェアで他のインタフェースと共存できません）。DSL モデムをインタフェースネットワークセグメントに接続する必要があります。これらのデバイスタイプのネットワークパラメータは、リモートステーション（使用しているISP など）で割り当てることができます。さらに、ISP アカウントのユーザ名およびパスワードを入力する必要があります。

イーサネット DHCP:これは DHCP を使用した標準イーサネットインタフェースです。

イーサネットスタティック:これは標準のイーサネットインターフェースで、10、100、あるは1000Mbps の帯域幅があります。

イーサネット VLAN:VLAN（仮想 LAN）は、単一のハードウェアインタフェース上に別個のレイヤ2 ネットワークセグメントを複数持つ方式です。各セグメントは整数の「タグ」で識別されます。VLAN インタフェースを追加することで、インタフェース（エイリアス）の追加に使用できる「ハードウェア」デバイスが作成されます。PPPoE および PPPoA デバイスは、VLAN 仮想ハードウェア上では実行できません。

モデム (PPP):このタイプのインタフェースでは、PPP モデムを介して UTM をインターネットに接続できます。設定には、UTM にシリアルインタフェースと外部モデムが必要です。また、ユーザ名とパスワードを含むDSL アクセスデータも必要です。これらのデータは、使用しているISP から入手できます。

フレキシブルスロットについて

一部の Sophos ハードウェアアプライアンスにあるスロットを使用して、容易にハードウェアインタフェースを変更することができます。スロットモジュールを挿入し、柔軟に切り替えることができます。そのようなハードウェアを使用している場合、WebAdmin では、各ハードウェアインターフェースに対して、スロット情報も表示されます。たとえば、*eth1 [A6] Intel Corporation 82576 Gigabit Network Connection* などと表示されます。ここで、スロット情報は角括弧で囲まれ、*A6* は、スロット A の 6番目のポートを指します。現在、最高 3種類のスロット（A、B、C）があり、各スロットに対して最高 8種

類のポートがあります。オンボードタイプのインターフェースカードは、*[MGMT1]* および *[MGMT2]* と表示されます。

スロット情報は、WebAdmin の次の場所で表示されます。

- *インターフェースとルーティング > インターフェース > インターフェース*
- *インターフェースとルーティング > インターフェース > ハードウェア*
- WebAdmin にある、すべての「*ハードウェア*」ドロップダウンリスト、およびハードウェアインターフェース情報が表示されているリスト。

フレキシブルスロットが装備されているアプライアンスの種類の最新情報は、Sophos UTM Web ページ を参照してください。

6.1.1.3 グループ

2つ以上のインタフェースをグループにまとめることができます。グループ化により、設定タスクを簡素化することができます。マルチパスルールを作成する場合に、すべてのアップリンクインタフェースではなく、定義したアップリンクインタフェースグループでのみトラフィックの分散を行うには、グループを設定する必要があります。

「*グループ*」インタフェースを設定するには、次の手順に従います。

1. **「*インタフェース*」タブで、「*新規インタフェース*」をクリックします。**

   「*新規インタフェースの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:インタフェースを説明する名前を入力してください。

   タイプ:ドロップダウンリストから「*グループ*」を選択します。

   インタフェース:グループ化するインタフェースを追加します。

   コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   グループがインタフェースリストに追加されます。グループにステータスはありません。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.4 3G/UMTS

Sophos UTM は、3G/UMTS USB モデムスティックを使用したネットワーク接続をサポートしています。

3G/UMTS インタフェースを設定するには、次の手順に従います。

1. **「*インタフェース*」タブで、「*新規インタフェース*」をクリックします。**

   「*新規インタフェースの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:インタフェースを説明する名前を入力してください。

   タイプ:ドロップダウンリストから「*3G/UMTS*」を選択します。

   ハードウェア:ドロップダウンリストから USB モデムスティックを選択します。USB モデムスティックを差し込んだ後で、再起動する必要があります。

   ネットワーク:モバイルネットワークの種類を、*GSM/W-CDMA*、*CDMA*、または *LTE* から選択します。

   IPv4/IPv6 デフォルトG/W(任意):プロバイダのデフォルトゲートウェイを使用する場合、このオプションを選択します。

   PIN(任意):PIN が設定されている場合、SIM カードの PIN を入力します。

   APN 自動選択:(任意):デフォルトで、使用する APN(アクセスポイント名)は USB モデムスティックから取得されます。チェックボックスの選択を外す場合は、「*APN*」フィールドに APN 情報を入力します。

   ユーザ名/パスワード(任意):必要な場合、モバイルネットワークのユーザ名とパスワードを入力します。

   ダイヤル文字列(任意):プロバイダが異なるダイヤル文字列を使用している場合、ここに入力します。デフォルトは `*99#` です。

   コメント(任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   初期化文字列:USB モデムスティックを初期化するための文字列を入力します。USB モデムスティックに応じて初期化文字列の変更が必要になる可能性があります。この場合、初期化文字列は当該 USB モデムスティックのマニュアルで確認できます。必要なマニュアルがない場合、デフォルトの *ATZ* を指定してください。

リセット文字列:USB モデムスティックのリセット文字列を入力します。USB モデムスティックに応じてリセット文字列の変更が必要になる可能性があります。この場合、リセット文字列は当該 USB モデムスティックのマニュアルで確認できます。必要なマニュアルがない場合、デフォルトの *ATZ* を指定してください。

MTU:インタフェースの最大伝送単位をバイト単位で入力します。トラフィック管理機能を使用するには、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して適切な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超える MTU サイズを指定する場合は、通信事業者およびネットワークカードがそれに対応している必要があります(例: ギガビットインタフェース)。デフォルトで、*3G/UMTS* インタフェースタイプには、1500バイトの MTU が設定されています。

非対称(任意):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させる場合は、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅を Mbps または Kbps 単位で入力します。ドロップダウンリストから適切な単位を選択します。

表示する最大速度(任意):ダッシュボードに表示する、接続の最大ダウンリンク帯域幅を入力します。帯域幅は Mbps または Kbps 単位で入力できます。ドロップダウンリストから適切な単位を選択します。

4. **「*保存*」をクリックします。**
   システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(トグルスイッチはグレー表示)。

5. **インタフェースを有効にします。**
   インタフェースを有効にするには、トグルスイッチをクリックします。

   これでインタフェースが有効になります(トグルスイッチは緑色)。インタフェースがまだ「*無効*」と表示される場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。「*有効*」が表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.5 イーサネットスタティック

内部または外部ネットワークに、スタティックイーサネット接続するためのネットワークカードを設定するには、IP アドレスとネットマスクを設定する必要があります。

スタティックイーサネットインタフェースを設定するには、次の手順に従ってください。

1. **「*インタフェース*」タブで、「*新規インタフェース*」をクリックします。**

   「*新規インタフェースの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:インタフェースを説明する名前を入力してください。

   タイプ:ドロップダウンリストから「*イーサネットスタティック*」を選択します。

   ハードウェア:ドロップダウンリストからインタフェースを選択します。

   > **ヒント –** インターネットなどの外部接続には、SysID が eth1 のネットワードカードを選択してください。1枚のネットワークカードを、*イーサネットスタティック*インタフェースおよび *PPPoE DSL (PPP over Ethernet)* 接続または *PPPoA DSL (PPTP over Ethernet)* 接続として同時に使用することはできません。

   IPv4/IPv6 アドレス:インターフェースの IP アドレスを入力します。

   ネットマスク:ネットワークマスク(IPv4)を選択するか、IPv6 ネットワークマスクを入力します。

   IPv4/IPv6 デフォルトG/W(任意):スタティックに定義されたデフォルトゲートウェイを使用するには、このオプションを選択します。

   デフォルトG/W IP(任意):デフォルトゲートウェイ の IP アドレスを入力します。

   > **注 –** IPv4 および IPv6 アドレスを同時に使用するよう、インタフェースを設定することができます。

   コメント(任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   MTU:インタフェースの最大伝送単位をバイト単位で入力します。トラフィック管理機能を使用するには、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して適切な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェース

が使用不可能になる場合があります。1500バイトを超えるMTUサイズを指定する場合は、通信事業者およびネットワークカードがそれに対応している必要があります(例: ギガビットインタフェース)。デフォルトで、「*イーサネットスタティック*」インタフェースタイプには1500バイトのMTUが設定されています。

プロキシARP:この機能を有効にするには、チェックボックスを選択します。デフォルトで、「*プロキシARP*」機能は無効になっています。
このオプションはブロードキャストタイプのインタフェースで使用できます。これを選択すると、UTMは、インタフェース上のトラフィックを、その「背後にある」ホストの代わりに「引きつけ」、渡します。直接接続されたインタフェースルートがあるすべてのホストに対してこの処理が行われます。これにより、ファイアウォールを実行したまま、「透過的な」ネットワークブリッジを構築することができます。この機能の他の利用方法としては、ISPのルータが「公式」ネットワークのみをイーサネットインタフェースに受け入れる場合があります(ホストルートを使用しない)。

非対称(任意):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させる場合は、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切な単位を選択します。

表示する最大速度(任意):ダッシュボードに表示する、接続の最大ダウンリンク帯域幅を入力します。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切な単位を選択します。

4. **「*保存*」をクリックします。**
システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(トグルスイッチはグレー表示)。

5. **インタフェースを有効にします。**
インタフェースを有効にするには、トグルスイッチをクリックします。

これでインタフェースが有効になります(トグルスイッチは緑色)。インタフェースがまだ「*無効*」と表示される場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。「*有効*」が表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.6 イーサネット VLAN

UTM を仮想 LAN に接続するためには、タグ付け可能なドライバのあるネットワークカードが必要になります。タグとは、イーサネットヘッダの一部としてパケットに付けられる 4バイトのヘッダです。タグには、パケットの送信先となる VLAN の番号が格納されます。VLAN の番号は 12ビット数で、最大 4095の仮想 LAN まで許可します。WebAdmin では、この数を「*VLAN タグ*」と呼びます。

注 – Sophos は、タグ付け可能なネットワークインタフェースカードのリストを管理しています。*ハードウェア互換性リスト*(HCL)は Sophos サポートデータベースから利用可能です。「HCL」を検索用語として使用して、該当するページを探してください。

イーサネット VLAN インタフェースを設定するには、次の手順に従ってください。

1. **「*インタフェース*」タブで、「*新規インタフェース*」をクリックします。**

   「*新規インタフェースの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:インタフェースを説明する名前を入力してください。

   タイプ:ドロップダウンリストから「*イーサネット VLAN*」を選択します。

   ハードウェア:ドロップダウンリストからインタフェースを選択します。

   VLAN タグ:このインタフェースに対して使用する VLAN タグを入力します。

   IPv4/IPv6 アドレス:インターフェースの IP アドレスを入力します。

   ネットマスク:ネットワークマスク(IPv4)を選択するか、IPv6 ネットワークマスクを入力します。

   IPv4/IPv6 デフォルトG/W(任意):スタティックに定義されたデフォルトゲートウェイを使用するには、このオプションを選択します。

   デフォルトG/W IP(任意):デフォルトゲートウェイ の IP アドレスを入力します。

   注 – IPv4 および IPv6 アドレスを同時に使用するよう、インタフェースを設定することができます。

   コメント(任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   MTU:インタフェースの最大伝送単位をバイト単位で入力します。トラフィック管理機能を使用するには、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して適切な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超えるMTUサイズを指定する場合は、通信事業者およびネットワークカードがそれに対応している必要があります(例: ギガビットインタフェース)。デフォルトで、「*イーサネット VLAN*」インタフェースタイプには1500バイトのMTUが設定されています。

   プロキシ ARP:この機能を有効にするには、チェックボックスを選択します。デフォルトで、「*プロキシ ARP*」機能は無効になっています。
   このオプションはブロードキャストタイプのインタフェースで使用できます。これを選択すると、UTMは、インタフェース上のトラフィックを、その「背後にある」ホストの代わりに「引きつけ」、渡します。直接接続されたインタフェースルートがあるすべてのホストに対してこの処理が行われます。これにより、ファイアウォールを実行したまま、「透過的な」ネットワークブリッジを構築することができます。この機能の他の利用方法としては、ISP のルータが「公式」ネットワークのみをイーサネットインタフェースに受け入れる場合があります(ホストルートを使用しない)。

   非対称(任意):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させる場合は、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切な単位を選択します。

   表示する最大速度(任意):ダッシュボードに表示する、接続の最大ダウンリンク帯域幅を入力します。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切な単位を選択します。

4. **「保存」をクリックします。**
   システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(トグルスイッチはグレー表示)。

5. **インタフェースを有効にします。**
   インタフェースを有効にするには、トグルスイッチをクリックします。

   これでインタフェースが有効になります(トグルスイッチは緑色)。インタフェースがまだ「*無効*」と表示される場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。「*有効*」が表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.7 イーサネット DHCP

*イーサネット DHCP*インタフェースを設定するには、次の手順に従ってください。

1. **「*インタフェース*」タブで、「*新規インタフェース*」をクリックします。**

   「*新規インタフェースの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:インタフェースを説明する名前を入力してください。

   タイプ:ドロップダウンリストから「*イーサネット DHCP*」を選択します。

   ハードウェア:ドロップダウンリストからインタフェースを選択します。

   ヒント – インターネットなどの外部接続には、SysID が `eth1` のネットワークカードを選択してください。1枚のネットワークカードを、*イーサネット DHCP* および*PPP over Ethernet* (PPPoE-DSL) または *PPTP over Ethernet* (PPPoA-DSL) 接続として同時に使用することはできません。

   IPv4/IPv6 デフォルトG/W (任意):プロバイダのデフォルトゲートウェイを使用する場合、このオプションを選択します。

   コメント (任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   ホスト名:ISP がシステムのホスト名の受信を要求する場合、ここに入力します。

   MTU:インタフェースの最大伝送単位をバイト単位で入力します。トラフィック管理機能を使用するには、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して適切な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超える MTU サイズを指定する場合は、通信事業者およびネットワークカードがそれに対応している必要があります (例: ギガビットインタフェース)。デフォルトで、「*イーサネット DHCP*」インタフェースタイプには 1500バイトの MTU が設定されています。

プロキシ ARP:この機能を有効にするには、チェックボックスを選択します。デフォルトで、「*プロキシ ARP*」機能は無効になっています。
このオプションはブロードキャストタイプのインタフェースで使用できます。これを選択すると、UTM は、インタフェース上のトラフィックを、その「背後にある」ホストの代わりに「引きつけ」、渡します。直接接続されたインタフェースルートがあるすべてのホストに対してこの処理が行われます。これにより、ファイアウォールを実行したまま、「透過的な」ネットワークブリッジを構築することができます。この機能の他の利用方法としては、ISP のルータが「公式」ネットワークのみをイーサネットインタフェースに受け入れる場合があります(ホストルートを使用しない)。

非対称(任意):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させる場合は、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅を Mbps または Kbps 単位で入力します。ドロップダウンリストから適切な単位を選択します。

表示する最大速度(任意):ダッシュボードに表示する、接続の最大ダウンリンク帯域幅を入力します。帯域幅は Mbps または Kbps 単位で入力できます。ドロップダウンリストから適切な単位を選択します。

4. **「*保存*」をクリックします。**
システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(トグルスイッチはグレー表示)。

5. **インタフェースを有効にします。**
インタフェースを有効にするには、トグルスイッチをクリックします。

これでインタフェースが有効になります(トグルスイッチは緑色)。インタフェースがまだ「*無効*」と表示される場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。「*有効*」が表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.8 DSL (PPPoE)

設定には、ご利用の ISP が提供したユーザ名とパスワードを含む DSL 接続情報が必要になります。VDSL もこのインタフェースタイプでサポートされています。

注 – DSL 接続を有効にすると、UTMはご利用の ISP に 1日 24時間接続されます。したがって、ご利用の ISP の請求が接続時間ベースではなく定額制または帯域幅ベースの料金システムであることをご確認ください。

DSL（PPPoE）インタフェースを設定するには、次の手順に従ってください。

1. **「*インタフェース*」タブで、「*新規インタフェース*」をクリックします。**

   「*新規インタフェースの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:インタフェースを説明する名前を入力してください。

   タイプ:ドロップダウンリストから「*DSL (PPPoE)*」を選択します。

   ハードウェア:ドロップダウンリストからインタフェースを選択します。

   VDSL:このチェックボックスは、使用中の接続が VDSL 接続である場合のみ選択します。*MTU* は `1476` に変更されます。

   スタティック PPPoE IP（任意）:ISP に割り当てられたスタティック IP アドレスがある場合、チェックボックスにチェックを入れ、表示されるテキストボックスに IP アドレスと該当するネットマスクを入力します。

   - **IPv4/IPv6 アドレス:**インターフェースの IP アドレスを入力します。
   - **ネットマスク:**ドロップダウンリストからネットマスクを選択するか、または IPv6 ネットマスクを入力します。

   注 – インタフェースを設定して、IPv4 および IPv6 アドレスを同時に使用することができます。

   IPv4/IPv6 デフォルト G/W（任意）:プロバイダのデフォルトゲートウェイを使用する場合、このオプションを選択します。

   ユーザ名:ISP から入手したユーザ名を入力します。

   パスワード:ISP から入手したパスワードを入力します。

   コメント（任意）:説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
MTU:インタフェースの最大伝送単位をバイト単位で入力します。トラフィック管理機能を使用するには、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して適切な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超えるMTUサイズを指定する場合は、通信事業者およびネットワークカードがそれに対応している必要があります(例: ギガビットインタフェース)。デフォルトで、「*DSL (PPPoE)*」インタフェースタイプには1492バイトのMTUが設定されています。

VLANタグ(*VDSL*が有効な場合のみ):PPPoEパケットに追加するVLANタグを入力します。該当するタグの詳細は、VDSLプロバイダにお問い合わせください。デフォルトは7で、現在Deutsche TelekomのPPPoE接続に使用されています。

日次再接続:接続を終了および再開する時間を定義します。「*なし*」を選択するか、具体的な時間を指定することができます。

再接続ディレイ:ここで、再接続ディレイを変更できます。デフォルトでは、「*5秒*」に設定されています。ご利用のISPがこれより長い遅延を要求している場合は、「*1分*」や「*15分*」に設定できます。

非対称(任意):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させる場合は、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅をMbpsまたはKbps単位で入力します。ドロップダウンリストから適切な単位を選択します。

表示する最大速度(任意):ダッシュボードに表示する、接続の最大ダウンリンク帯域幅を入力します。帯域幅はMbpsまたはKbps単位で入力できます。ドロップダウンリストから適切な単位を選択します。

マルチリンク:有効にすると、複数のPPP接続を1つにまとめることができます。マルチリンクのPPP接続は、使用しているISPがマルチリンクPPPに対応している場合のみ動作します。

マルチリンクスレーブ:先ほど選択したハードウェアと1つのマルチリンクにまとめるインターフェースを選択します。

4. **「*保存*」をクリックします。**
システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(トグルスイッチはグレー表示)。

5. **インタフェースを有効にします。**
   インタフェースを有効にするには、トグルスイッチをクリックします。

   これでインタフェースが有効になります(トグルスイッチは緑色)。インタフェースがまだ「*無効*」と表示される場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。「*有効*」が表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.9 DSL (PPPoA/PPTP)

PPPoA (*PPP over ATM Protocolプロトコル*)した接続を設定するには、UTM上の未使用のイーサネットインタフェースと、イーサネットポート付きの外部 ADSL モデムが必要です。インターネットへの接続は2つの個別の接続で行ないます。UTMとADSLモデム間では、*PPTP over Ethernet プロトコル*を使用して接続を確立します。ADSL モデムは、*PPP over ATM Dialing プロトコル*を使用して ISP に接続します。

設定には、ご利用のインターネットサービスプロバイダ (ISP) が提供したユーザ名とパスワードを含む DSL 接続情報が必要になります。

注 – DSL 接続を有効にすると、UTMはご利用の ISP に 1日 24時間接続されます。したがって、ご利用の ISP の請求が接続時間ベースではなく定額制または帯域幅ベースの料金システムであることをご確認ください。

DSL (PPPoA/PPTP) インタフェースを設定するには、次の手順に従ってください。

1. **「*インタフェース*」タブで、「*新規インタフェース*」をクリックします。**

   「*新規インタフェースの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:インタフェースを説明する名前を入力してください。

   タイプ:ドロップダウンリストから「*DSL (PPPoA/PPTP)*」を選択します。

   ハードウェア:ドロップダウンリストからインタフェースを選択します。

   IPv4 デフォルトG/W (任意):プロバイダのデフォルトゲートウェイを使用する場合、このオプションを選択します。

   ユーザ名:ISP から入手したユーザ名を入力します。

パスワード:ISP から入手したパスワードを入力します。

コメント(任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
モデム IP:使用している ADSL モデムの IP アドレスをここに入力します。このアドレスは通常、ISP から、あるいはモデムハードウェアとともに提供されるので、変更できません。
例:`10.0.0.138`(AonSpeed)。

NIC アドレス:モデムに接続されている UTM 上のネットワークカードの IP アドレスをここに入力します。このアドレスはモデムと同じサブネット内にある必要があります。例:`10.0.0.140`(AonSpeed)。

NIC ネットマスク:使用するネットワークマスクをここに入力します。
例:`255.255.255.0`(AonSpeed)。

Ping 先アドレス(任意):ICMP ping 要求に応答するインターネット上のホストの IP アドレスを入力します。UTM と外部ネットワーク間の接続をテストするには、PPTP リンクの反対側ホストの IP アドレスを入力する必要があります。使用している ISP の DNS サーバを指定できます。UTMがこのホストに ping 要求を送信します。応答がない場合は、接続不良です。

MTU:インタフェースの最大伝送単位をバイト単位で入力します。トラフィック管理機能を使用するには、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して適切な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超える MTU サイズを指定する場合は、通信事業者およびネットワークカードがそれに対応している必要があります(例: ギガビットインタフェース)。デフォルトで、「*DSL (PPPoA)*」インタフェースタイプには 1492 バイトの MTU が設定されています。

日次再接続:接続を終了および再開する時間を定義します。「*なし*」を選択するか、具体的な時間を指定することができます。

再接続ディレイ:ここで、再接続ディレイを変更できます。デフォルトでは、「*5秒*」に設定されています。ご利用の ISP がこれより長い遅延を要求している場合は、「*1分*」や「*15分*」に設定できます。

非対称(任意):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させる場合は、このオプションを選択します。選択すると、2つのテキストボックスが表示されます。ここに最大アップリンク帯域幅を Mbps または Kbps 単位で入力します。ドロップダウンリストから適切な単位を選択します。

表示する最大速度(任意):ダッシュボードに表示する、接続の最大ダウンリンク帯域幅を入力します。帯域幅は Mbps または Kbps 単位で入力できます。ドロップダウンリストから適切な単位を選択します。

4. **「*保存*」をクリックします。**
システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(トグルスイッチはグレー表示)。

5. **インタフェースを有効にします。**
インタフェースを有効にするには、トグルスイッチをクリックします。

これでインタフェースが有効になります(トグルスイッチは緑色)。インタフェースがまだ「*無効*」と表示される場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。「*有効*」が表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.1.10 モデム(PPP)

設定には、UTMにシリアルインタフェースと外部 PPP モデムが必要になります。また、ユーザ名とパスワードを含む DSL アクセスデータも必要です。これらのデータは、インターネットサービスプロバイダ(ISP)から入手できます。

*モデム(PPP)*インタフェースを設定するには、次の手順に従ってください。

1. **「*インタフェース*」タブで、「*新規インタフェース*」をクリックします。**

「*新規インタフェースの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
名前:インタフェースを説明する名前を入力してください。

タイプ:ドロップダウンリストから「*モデム(PPP)*」を選択します。

ハードウェア:ドロップダウンリストからインタフェースを選択します。

IPv4 デフォルトゲートウェイ(任意):プロバイダのデフォルトゲートウェイを使用する場合、このオプションを選択します。

ユーザ名:ISP から入手したユーザ名を入力します。

パスワード:ISP から入手したパスワードを入力します。

ダイヤル文字列:電話番号を入力します。例:5551230

コメント(任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
回線速度:UTM とモデムの間の接続に対して、速度を bps 単位で設定します。一般的な値は 57,600 bps と 115,200 bps です。

フローコントロール:データフローをコントロールする方法を選択します。
データがシリアル接続経由で転送される場合、システムで受信データを十分に速く処理できない可能性があります。データの損失が発生しないようにするためには、データフローのコントロール方法が必要になります。シリアル接続では、次の 2つの方法を使用できます。

- *ハードウェア*信号
- *ソフトウェア*信号

PPP 接続では、すべての 8ビットがデータ転送回線に使用され、転送されるデータにはコマンドサイン *Control S*と *Control Q* のバイトが含まれるため、デフォルト設定の「*ハードウェア*」を維持し、シリアル接続ケーブルを使用することをお勧めします。

初期化文字列:モデムを初期化するための文字列を入力します。モデムに応じて初期化文字列の調整が必要になる可能性があります。この場合、初期化文字列は該当モデムのマニュアルで確認できます。必要なマニュアルがない場合、デフォルトの *ATZ*を指定してください。

リセット文字列:モデムのリセット文字列を入力します。モデムに応じてリセット文字列の調整が必要になる可能性があります。この場合、リセット文字列は該当モデムのマニュアルで確認できます。必要なマニュアルがない場合、デフォルトの *ATZ*を指定してください。

MTU:インタフェースの最大伝送単位をバイト単位で入力します。トラフィック管理機能を使用するには、インタフェースタイプに対応する値をここに入力する必要があります。インタフェースタイプに対して適切な値がデフォルトで入力されています。この設定の変更は、技術的に熟練したユーザのみが行ってください。ここに不正な値を入力すると、インタフェースが使用不可能になる場合があります。1500バイトを超える MTU サイズを指定する場合は、通信事業者およびネットワークカードがそれに対応している必要があります(例: ギガビットインタフェース)。デフォルトで、モデム *(PPP)*インタフェースタイプには 1492バイトの MTU が設定されています。

非対称(任意):接続のアップリンクとダウンリンクの帯域幅が同一でない場合に、ダッシュボードにこれを反映させる場合は、このオプションを選択します。選択すると、2つのテキスト

ボックスが表示されます。ここに最大アップリンク帯域幅を Mbps または Kbps 単位で入力します。ドロップダウンリストから適切な単位を選択します。

表示する最大速度(任意):ダッシュボードに表示する、接続の最大ダウンリンク帯域幅を入力します。帯域幅は Mbps または Kbps 単位で入力できます。ドロップダウンリストから適切な単位を選択します。

4. **「*保存*」をクリックします。**
システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(トグルスイッチはグレー表示)。

5. **インタフェースを有効にします。**
インタフェースを有効にするには、トグルスイッチをクリックします。

これでインタフェースが有効になります(トグルスイッチは緑色)。インタフェースがまだ「*無効*」と表示される場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。「*有効*」が表示されたら、インタフェースは完全に動作可能です。

特定タイプのインタフェースのみ表示する場合は、ドロップダウンリストから表示するインタフェースのタイプを選択します。インタフェースを編集または削除するには、対応するボタンをクリックします。

6.1.2 追加アドレス

1つのネットワークカードで追加 IP アドレス(別名「*エイリアス*」)を設定できます。この機能を使用すると、1つの物理ネットワークカード上で複数の論理ネットワークを管理することができます。また、これを使用して、UTMNAT(ネットワークアドレス変換)を実行している にさらなるアドレスを割り当てることもできます。

標準イーサネットインタフェースで追加アドレスを設定するには、次の手順に従ってください。

1. **「*追加アドレス*」タブで、「*新規追加アドレス*」をクリックします。**
「*新規追加アドレスの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
名前:新しい追加アドレスを説明する名前を入力してください。

インタフェース:アドレスを割り当てるインタフェースをドロップダウンリストから選択します。

IPv4/IPv6 アドレス:インターフェースの追加 IP アドレスを入力します。

ネットマスク:ドロップダウンリストからネットマスクを選択するか、または IPv6 ネットマスクを入力します。

注 – IPv4 および IPv6 アドレスを同時に使用するよう、インタフェースを設定することができます。

コメント(任意):説明などの情報を追加します。

3. **「保存」をクリックします。**
システムが設定の有効性を確認します。チェックに成功すると、新しいインタフェースがインタフェースリストに表示されます。インタフェースはまだ有効ではありません(トグルスイッチはグレー表示)。

4. **追加アドレスを有効にします。**
追加アドレスを有効にするには、トグルスイッチをクリックします。

これで追加アドレスが有効になります(トグルスイッチは緑)。追加アドレスはまだ*「ダウン(Down)」*と表示されている場合があります。システムが構成を行い、設定をロードするまで、しばらく時間がかかります。*「アップ(Up)」*というメッセージが表示されると、追加アドレスは完全に機能するようになっています。

追加アドレスを編集または削除するには、対応するボタンをクリックします。

6.1.3 リンクアグリゲーション

リンクアグリゲーションは、「ポートトランキング」または「NIC ボンディング」とも呼ばれ、これによって複数のイーサネットネットワークポートを1つの仮想インタフェースに集約することができます。集約されたポートはシステム上で1つの IP アドレスとして表示されます。リンクアグリゲーションは、どの単体 NIC よりも リンク速度を向上させたり、いずれかのポートまたはスイッチで障害が発生した場合に冗長性を維持して基本フェイルオーバーおよびフォールトトレランス機能を提供したりするために役に立ちます。障害が発生したポートやスイッチにルーティングされているすべてのトラフィックは自動的にリルートされ、残りのポートまたはスイッチのいずれかを使用するようになります。このフェイルオーバーは、接続を使用しているシステムに対して完全に透過的です。

注 – HA 環境では、イーサネット接続を別の HA ユニット上にすることもできます。

リンクアグリゲーショングループは最大 4つまで定義することができます。グループは 1つのインタフェースまたは複数のインターフェースで構成できます。

リンクアグリゲーショングループ(LAG)を作成するには、次の手順に従います。

1. **各 LAG に対して、追加するインタフェースを選択します。**
   グループは、設定されているインタフェースまたは 1つ以上の設定されていないインタフェース（あるいはその両方）で構成することができます。

   設定されているインタフェースを使用するには、「*変換インタフェース*」ドロップダウンリストからインタフェースを選択します。設定されていないインタフェースを使用するには、それぞれのチェックボックスにチェックを入れます。

2. **LAGを有効にします。**
   「*このグループを有効化*」ボタンをクリックして、グループを有効にします。

   リンクアグリゲーショングループを設定すると、「*インタフェース*」タブでインタフェース定義を作成するときに、新しい LAG インタフェース（`lag0` など）を選択できるようになります。ボンディングインタフェースの上部で、次のいずれかを作成できます。

   - イーサネットスタティック
   - イーサネット VLAN
   - イーサネット DHCP
   - エイリアスインタフェース

LAG を無効にするには、LAG を構成するインタフェースのチェックボックスのチェックを外して、「*このグループを更新*」をクリックし、警告メッセージを確認します。LAG インタフェースのステータスが、「*サポート > 詳細 > インタフェーステーブル*」タブに表示されます。

6.1.4 アップリンクバランシング

アップリンクバランシング機能を使用すると、複数のインターネットアップリンクを組み合わせて、バックアップ用アップリンクを使用可能にするか、複数のアップリンクに負荷を分散することができます。組み合わせることができるアップリンクは最大32です。ベーシックガード サブスクリプションでは、組み合わせることのできるアップリンクは 2つのみであることに注意してください。

デフォルトゲートウェイを備えた既存インタフェースに加えて、デフォルトゲートウェイをインタフェースに割り当てると、アップリンクバランシングが自動的に有効になります。デフォルトゲートウェイを装備するすべてのインタフェースは、「*アクティブインタフェース*」ボックスに追加され、以降はアップリンクバランシングにより、これらのインタフェースの間で自動的にバランシングが行われます。デフォルトゲートウェイを装備する他のインタフェースもすべて自動的に追加されます。

「*マルチパスルール*」タブでは、トラフィックのバランシングを行うための特定ルールを定義できます。

アップリンクバランシングを手動でセットアップするには、次の手順に従います。

1. **アップリンクバランシングを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*アップリンクバランス*」エリアが編集可能になります。

2. **アクティブインタフェースを選択します。**
   フォルダアイコンをクリックしてインタフェースを1つ以上追加し、オブジェクトリストからインタフェースをドラッグします。インターフェースが複数ある場合、クライアントから送信されるトラフィックのバランシングは、送信元に基づいて行われます。つまり、1つの送信元から送られたトラフィックはすべて同じインタフェースを使用する一方で、別の送信元からのトラフィックは別のインタフェースに送信できます。いずれかのインタフェースを使用できない場合、トラフィックは残りのインタフェースによってテイクオーバーされます。

   注 – 最初にアップリンクバランシングが自動的に有効化された段階で、「*アクティブインタフェース*」リストには既にデフォルトゲートウェイを装備するすべてのインタフェースが表示されます。リストからインタフェースを削除すると、インタフェースの「*デフォルトゲートウェイ*」チェックボックスから自動的にチェックが外れます。したがって、デフォルトゲートウェイを装備するすべてのインタフェースは、このリストに示されるか、その下の「*スタンバイインタフェース*」ボックスに示されるかのいずれかになります。しかし、デフォルトゲートウェイを装備しないインタフェースを追加して、後にデフォルトゲートウェイのアドレスを入力することができます。

   注 – インタフェースの順序は重要な意味を持ちます。1つのインターフェースのみ使用できる設定で、UTM 自身から送信されるパケットの場合、1つ目のアクティブなインターフェースがデフォルトで使用されます。インタフェースの順序は、ボックス内の並び替えアイコンをクリックして変更します。

   ボックスのヘッダの「スケジューラの編集」ボタンを使用すると、個々のバランシング動作およびアクティブインタフェースのインタフェースパーシスタンスを設定することができます。

   加重:加重とは、あるインタフェースが処理するトラフィック量を他のインタフェースに対して相対的に示すもので、0～100 の間で設定できます。加重ラウンドロビンアルゴリズムが使用され、値が大きいほど、該当インタフェースにルーティングされるトラフィックが多くなります。相対的な値であるため、合計して 100 にする必要はありません。たとえば、インタフェース 1 の値を 100 に、インタフェース 2 の値を 50 に、インタフェース 3 の値を 0 に設定することなどができます。この場合、インタフェース 2 のトラフィック量はインタフェース 1 の半分となり、インタフェース 3 は他のインタフェースが使用可能でない場合にのみ使用されます。0 の

値は、より値が大きい他のインタフェースが常に使用されることを示します(他のインタフェースが使用可能であれば)。

パーシスタンス:インタフェースパーシスタンスとは、特定の属性を持つトラフィックが常に同じアップリンクインタフェース経由でルーティングされるようにする技術です。パーシスタンスのデフォルトのタイムアウト時間は1時間です。

3. **スタンバイインタフェースの選択 (Select standby interfaces)**(オプション)
ここでは、すべてのアクティブインタフェースが使用不能になった場合にのみ使用されるフェイルオーバーインタフェースをオプションで追加することができます。この場合、表示されている順番の最初のスタンバインターフェースが使用されます。インタフェースの順序は、ボックス内の並び替えアイコンをクリックして変更します。

4. **モニタリング設定の変更**(任意)。
デフォルトでは、インタフェース障害の可能性を検出するために「*自動モニタリング*」が有効になっています。つまり、すべてのアップリンク バランシング インタフェースからインターネット上の特定のホストに 15秒間隔で接続することにより、それらのインタフェースの状態(健全性)がモニタリングされます。デフォルトでは、ホストのモニタリングは、1つのルート DNS サーバまでのルート上にある、ping を許可する 3番目のホップです。なお、ユーザはサーバプールをモニタリングするためのホストを自分で定義することができます。これらのホストには、ping 以外の別のサービスを選択し、モニタリング間隔とタイムアウトを変更できます。

   モニタリングホストが応答を送信しなくなった場合、そのインタフェースは機能していないと見なされるため、それ以降配信に使用されません。ダッシュボードでは、インタフェースの「*リンク*」列に「エラー」と表示されます。

   注 – 同じモニタリング設定が、アップリンクモニタリング(*アップリンクモニタリング > 詳細*)とアップリンクバランシング(*インターフェース > アップリンクバランシング*)に対して使用されます。

   サーバプールをモニタリングするホストを手動で定義するには、次の操作を行ってください。

   1. **「*自動モニタリング*」チェックボックスのチェックを外します。**
   「*モニタリングホスト*」ボックスが編集可能になります。

   2. **モニタリングホストを追加します。**
   任意のホストを使用する代わりに、モニタリングに使用するホストを 1つ以上追加します。複数のホストでインタフェースをモニタリングする場合、定義された時間内にすべてのモニタリングホストが応答しない場合にのみ、インタフェースがデッド(dead)とみなされます。

注 – 選択したホストがインタフェースに関連付けられている場合は、このインタフェースのモニタリングのみに使用されます。ホストがインタフェースに関連付けられていない場合は、すべてのインタフェースのモニタリングに使用されます。選択したホストによりカバーされていないインタフェースは、自動モニタリングによりモニタリングされます。

ボックスのヘッダにある「モニタリング設定」アイコンをクリックすると、モニタリングの詳細を設定できます。

モニタリングタイプ:モニタリング用のサービスプロトコルを選択します。モニタリング用に「*TCP*」(TCP 接続の確立)、「*UDP*」(UDP 接続の確立)、「*Ping*」(ICMP Ping)、「*HTTP ホスト*」(HTTP 要求)、または「*HTTPS ホスト*」(HTTPS 要求)のいずれかを選択します。「*UDP*」を使用する場合、ping 要求が最初に送信され、成功した場合は、続いてペイロード 0 の UDP パケットが送信されます。ping が成功しなかった場合や、ICMP ポートに到達できない場合、この接続はダウンしているとみなされます。

ポート(「*TCP*」および「*UDP*」のモニタリングタイプ選択時のみ):要求の送信先のポート番号。

URL(任意。「*HTTP/S ホスト*」のモニタリングタイプ選択時のみ):要求する URL。URL にポート情報を追加することで、デフォルトのポート 80 または 443 以外のポートを使用できます(例: `http://example.domain:8080/index.html`)。URL を指定しない場合は、ルートディレクトリが要求されます。

間隔:ホストをチェックする間隔を秒単位で入力します。

タイムアウト:モニタリングホストが応答を送信する最大時間を秒単位で入力します。インタフェースのすべてのモニタリングホストがこの時間内に応答しない場合、インタフェースがデッド(dead)とみなされます。

3. **「*適用*」をクリックします。**
   設定が保存されます。

「*アップリンクインタフェース (Uplink Interfaces)*」という名前の新しい仮想ネットワークインタフェースが自動的に作成され、Sophos UTMの他の機能(IPsec ルールなど)で使用できるようになっています。仮想ネットワークインタフェース「*アップリンクインタフェース (Uplink Interfaces)*」は、インタフェースリストに追加されたすべてのアップリンクインタフェースから構成されています。
さらに、「*アップリンクプライマリアドレス (Uplink Primary Addresses)*」という名前の新しいネットワークグループが自動的に作成され、Sophos UTMの他の機能(ファイアウォールルールなど)で使

用できるようになっています。これは、すべての *アップリンクインタフェース*のプライマリアドレスを参照します。

DynDNS が使用されている場合や、リモートサーバがすべてのアップリンクインタフェースの IP アドレスを受け付けることができる場合は、インタフェースで障害が発生したときに、次に使用可能なインタフェースを介してオープンな VPN トンネルを自動的に再確立することができます。前提条件としては、IPsec ルールが「*ローカルインタフェース*」として「*アップリンクインタフェース*」を使用する必要があります。

6.1.5 マルチパスルール

「*インタフェース & ルーティング > インタフェース > マルチパスルール*」タブでは、アップリンクバランシング用のルールを設定できます。ルールは、トラフィックのバランシング（分散）を行うべき複数のインタフェースがある場合、「*アップリンクバランシング*」タブのアクティブインタフェースに適用されます。マルチパスルールがない場合、サービスはすべて送信元に基づいて分散されます。つまり、1つの送信元から送られたトラフィックはすべて同じインタフェースを使用する一方で、別の送信元からのトラフィックは別のインタフェースに送信できます。マルチパスルールを使用すると、このデフォルト設定のインタフェースパーシスタンスを変更することができます。

注 – マルチパスルールは、TCP、UDP、または IP タイプのサービスに対して設定できます。

マルチパスルールを作成するには、次の手順に従います。

1. **「*マルチパスルール*」タブで、「*新規マルチパスルール*」をクリックします。**
   「*新規マルチパスルールの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:マルチパスルールを説明する名前を入力してください。

   位置:位置番号。これによってルールの優先順位が定義されます。番号が小さいほど優先順位が高くなります。ルールは昇順に照合されます。あるルールが一致すると、それ以降、それより大きい番号のルールは評価されません。より具体的な帯域幅ルールをリストの上部に配置して、曖昧な帯域幅ルールが最後に照合されるようにします。

   送信元:照合する送信元 IP アドレスまたはネットワークを選択または追加します。

   サービス:照合するネットワークサービスを選択または追加します。

   宛先:照合する宛先 IP アドレスまたはネットワークを選択または追加します。

I/F パーシスタンス:*インタフェースパーシスタンス*とは、特定の属性を持つトラフィックが常に同じアップリンクインタフェース経由でルーティングされるようにする技術です。パーシスタンスのデフォルトのタイムアウト時間は1時間ですが、このタイムアウトは「*アップリンクバランシング*」タブで変更できます。何を基準にパーシスタンスを定めるかを定義することができます。

- **コネクション別:**(デフォルト)バランシングはコネクションに基づいて行われます。つまり、特定のコネクションに属するすべてのトラフィックが同じインタフェースを使用する一方で、別のコネクションのトラフィックは別のインタフェースに送信できます。
- **送信元別:**バランシングは送信元IPアドレスに基づいて行われます。つまり、1つの送信元から送られたすべてのトラフィックが同じインタフェースを使用する一方で、別の送信元からのトラフィックは別のインタフェースに送信できます。

  注 – プロキシを使用している場合、送信元に基づくパーシスタンスは実行できません。これは、オリジナルの送信元情報が維持されないことによります。なお、HTTP プロキシは例外です。HTTP プロキシによるトラフィックは、オリジナルのクライアント送信元 IP アドレスに一致するため、インターフェース パーシスタンス ルール「*送信元別*」に準拠します。

- **宛先別:**バランシングは宛先 IP アドレスに基づいて行われます。つまり、1つの宛先に送られるすべてのトラフィックが同じインタフェースを使用する一方で、別の宛先へのトラフィックは別のインタフェースに送信できます。
- **送信元/宛先別:**バランシングは送信元/宛先IPアドレスの組み合わせに基づいて行われます。つまり、送信元Aから宛先Bに送られるすべてのトラフィックが同じインタフェースを使用します。別の組み合わせのトラフィックは別のインタフェースに送信できます。上記の「注」も参照してください。
- **インタフェース別:**「*バインドインタフェース*」ドロップダウンリストからインタフェースを選択します。ルールに該当するすべてのトラフィックは、このインタフェース経由でルーティングされます。インタフェースで障害が発生し、後続のルールが一致しない場合、接続はデフォルトの動作にフォールバックします。

コメント(任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   分散先(インタフェースによるパーシスタンス以外):フィールドにインタフェースグループを追加します。ルールに該当するすべてのトラフィックは、このグループのインタフェースでバラ

ンシングされます。デフォルトでは、「*アップリンクインタフェース*が選択されるため、すべてのアップリンクインタフェースで接続がバランシングされます。

インタフェースエラーに関するルールをスキップ:これを選択すると、インターフェースで障害が発生した場合でも、トラフィックに対して、次に一致するマルチパスルールが使用されます。選択しない場合、インターフェースで障害が発生した場合でも、トラフィックに対して他のマルチパスルールが使用されません。これは、特定のスタティック IP アドレスのみから SMTP トラフィックを送信することで、無効な送信者 IP アドレスという原因で、送信したメールが受信者によってスパムとして分類されることを防ぐ場合などに便利です。

4. **「*保存*」をクリックします。**
   新しいマルチパスルールが「*マルチパスルール*」リストに追加されます。

5. **マルチパスルールを有効にします。**
   新しいルールはデフォルトで無効になっています（トグルスイッチはグレー表示）。ルールを有効にするには、トグルスイッチをクリックします。

   これでルールが有効になります（トグルスイッチは緑色）。

ルールを編集または削除するには、対応するボタンをクリックします。

6.1.6 ハードウェア

「*インタフェース & ルーティング > インタフェース > ハードウェア*」タブには、設定されているすべてのインタフェースが、イーサネットオペレーションモード、MAC アドレスなどの情報と共に表示されます。各 UTM ハードウェアデバイスの各インタフェースに対し、オートネゴシエーションを有効または無効にすることができます。

オートネゴシエーション:通常、2つのネットワークデバイス間のイーサネット操作モード（1000BASE-T 全二重、100BASE-T 全二重、100BASE-T 半二重、10BASE-T 全二重、10BASE-T 半二重など）が自動的にネゴシエートされ、両方のデバイスでサポートされる最適な操作モードが選択されます。このとき、速度は高速（1000Mbps など）が低速（100Mbps など）より優先され、同じ速度では全二重の方が半二重より優先されます。

警告 – 1000 Mbps のオペレーションを適切に機能させるためには、IEEE 標準 802.3ab により義務付けられているように、常にオートネゴシエーションが必要になります。このため、*リンクモード 1000BASE-T* のインタフェースの「*オートネゴシエーション*」を決してオフにしないようにしてください。ネットワークリンクにタイミング障害が発生して、サービスが低下したり、障害が発生する可能性があります。100 Mbps および 10 Mbps オペレーションでは、オートネゴシエーションがオプションですが、できる限り使用することを推奨します。

オートネゴシエーションはデフォルトで有効化されています。まれなケースでオートネゴシエーションをオフにする必要がある場合、対応するインタフェースカードの「*編集*」ボタンをクリックして、表示される「*NIC パラメータの編集*」ダイアログウィンドウ の「*リンクモード*」ドロップダウンリストで設定を変更します。ドロップダウンリストは、UTM ハードウェアデバイスのみで使用できます。「*保存*」をクリックして変更を保存します。

警告 – オートネゴシエーションを無効にするときは注意してください。これにより、不一致が生じ、パフォーマンスが大幅に低下したり、接続が切断したりする可能性もあります。該当するネットワークインタフェースカードが WebAdmin へのインタフェースである場合、WebAdmin へのアクセスが切断されてしまいます。

オートネゴシエーションや速度の変更の結果、インタフェースのネットワークリンクが失われた場合、設定を元に戻すだけでは、通常、インタフェースを通常の動作に戻すことはできません。切断されているインタフェースでは、オートネゴシエーションや速度を確実に変更することはできません。したがって、最初にオートネゴシエーションを有効にしてから UTM を再起動して通常の動作に戻します。

HA リンクモニタリング:冗長化が有効である場合、設定されたすべてのインタフェースでリンクステータスがモニタリングされます。リンクに障害が発生した場合、テイクオーバー（引き継ぎ）が行われます。設定されたインタフェースが常に接続されている訳ではない場合（管理インタフェースなど）、このインタフェースの HA リンクモニタリングは無効にしてください。無効にしないと、すべての HA リンクのステータスが「未接続（UNLINKED）」のままになります。HA リンクモニタリングを無効にするには、各インタフェースカードの「*編集*」ボタンをクリックして、表示される「*NIC パラメータの編集*」ダイアログウィンドウで設定を変更します。「*保存*」をクリックして変更を保存します。

仮想 MAC を設定:デバイスの MAC アドレスを変更できると便利な場合があります。たとえば、ISP によっては、モデムに接続されているデバイスに変更があった場合にこのモデムをリセットし、デバイスの MAC アドレスをリセットする必要があります。MAC アドレスを前のデバイスの値に設定することで、モデムのリセットを回避することができます。

UTMは、デバイスのオリジナルの MAC アドレスを上書きするのではなく、仮想 MAC アドレスを設定します。これを行うには、該当するインタフェースカードの「*編集*」ボタンをクリックします。表示される「*NIC パラメータの編集*」ダイアログウィンドウで、「*仮想 MAC の設定*」チェックボックスにチェックを入れ、有効な MAC アドレスを入力します。「*保存*」をクリックして変更を保存します。

オリジナルの MAC アドレスに復元するには、該当するインタフェースカードの「*編集*」ボタンをクリックします。表示される「*NIC パラメータの編集*」ダイアログウィンドウで、「*仮想 MAC の設定*」チェックボックスのチェックを外します。「*保存*」をクリックして変更を保存します。

6.2 ブリッジ

ブリッジングとは、主にイーサネットネットワークで使用されるパケット転送技術です。ルーティングと違い、ブリッジングでは特定のアドレスがネットワーク内のどこにあるのか推定するのではなく、ブロードキャスティングを使用して不明のデバイスを探します。

ブリッジングにより、複数のイーサネットネットワークまたはセグメントが相互接続できるようになります。データパケットはブリッジングテーブルを介して転送されます。ブリッジングテーブルは、ブリッジポートに MAC アドレスを割り当てます。作成されるブリッジは、ブリッジインタフェースを介してトラフィックを透過的に受け渡します。

注 – このようなトラフィックは、適切なファイアウォールルールによって明示的に許可する必要があります。

注 – ほとんどの仮想ホストのデフォルト設定では、仮想インタフェースでの MAC アドレスの変更や無差別モードを許可していません。仮想ホストでブリッジを機能させるには、仮想ホストの MAC アドレス検証を無効にしていることと、無差別モードを許可していることを確認してください。

6.2.1 ステータス

ブリッジを設定するには、次の手順に従ってください。

1. **「ステータス」タブでブリッジを有効にします。**
   「*インタフェースとルーティング* > *ブリッジ* > *ステータス*」タブで、トグルスイッチをクリックします。

   トグルスイッチンがアンバー色になり、「*ブリッジ設定*」エリアが編集可能になります。

2. **ブリッジングモードを選択します。**
   2種類のモードから選択可能です。

   - **全 NIC をブリッジ:**このオプションを選択すると、使用可能なすべてのイーサネット NIC（ネットワークインタフェースカード）がブリッジに加わります。このモードでは「*コンバートするインタフェース*」の指定が必須となります。コンバートするインタフェースを除くすべてのインタフェースが削除されます。
   - **一部の NIC をブリッジ:**ブリッジを形成する個々の NIC を選択できます。このためには、使用されていないネットワークインタフェースカードを用意する必要があります。

使用されていないネットワークインタフェースカードを 1つ以上選択してブリッジを形成します。また、新しいブリッジにコピーされる*コンバートするインタフェース*を指定することもできます。

3. **ブリッジにコンバートするインタフェースを選択します。**
   設定済みのインタフェースのみを選択できます。ブリッジは、そのインタフェースのアドレス設定と、追加アドレスおよび VLAN の設定を継承します。
4. **「*ブリッジの作成*」をクリックします。**
   ネットワークインタフェースが組み合わされ、ブリッジがアクティブになります(トグルスイッチが緑色になります)。

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

ブリッジの設定が完了すると、「*インタフェース & ルーティング* > *インタフェース*」タブに、コンバートされたインタフェースが SysID `br0` のブリッジデバイスとして表示されます。ブリッジのメンバであるすべてのインタフェースが「*ブリッジ設定*」エリアに表示されます。ブリッジからインタフェースを除外するには、チェックボックスからチェックを外して、「*ブリッジの更新*」をクリックします。

ブリッジを削除するには、次の手順に従ってください。

1. **「*ステータス*」タブで、トグルスイッチをクリックします。**
   トグルスイッチがアンバー色に変わります。
2. **「*ブリッジの削除を確認*」をクリックします。**
   トグルスイッチがグレーに変わります。ブリッジは正常に削除されました。

6.2.2 詳細

「*インタフェース & ルーティング* > *ブリッジ* > *詳細*」タブでは、次のブリッジオプションを設定できます。

ARP ブロードキャストを許可:この機能を使用すると、グローバル ARP ブロードキャストをブリッジで転送するかどうかを設定することができます。有効にすると、ブリッジは MAC 宛先アドレス `FF:FF:FF:FF:FF:FF` へのブロードキャストを許可します。ただし、これは疑わしい攻撃者に悪用され、各ネットワークセグメント内に導入されているネットワークカードや、場合によってはセキュリティ製品自体について、さまざまな情報を収集するために利用されてしまう危険性があります。そのため、デフォルト設定はこのようなブロードキャストがブリッジを通過できないようになっています。

スパニングツリープロトコル:このオプションを有効にすると、スパニングツリープロトコル(STP)が有効になります。このネットワークプロトコルは、ブリッジのループを検出して回避します。

警告 – スパニングツリープロトコルにはセキュリティ機能がないことが知られています。ですので、攻撃者はブリッジの構成を変えることができるかもしれません。

エージングタイムアウト:この時間（秒単位）が経過すると、無効な MAC アドレスは削除されます。デフォルト時間は 300秒です。

IPv6 パススルーを許可:このオプションを有効にすると、IPv6 トラフィックが検査を受けずにブリッジを通過できるようになります。

仮想 MAC アドレス:ここには、ブリッジの静的 MAC アドレスを入力できます。デフォルトでは（およびエントリが 00:00:00:00:00:00 の場合）、ブリッジがそのメンバのインタフェースの中で最も小さい MAC アドレスを使用します。

転送 EtherType:デフォルトでは、で設定されたブリッジは IP パケットのみを転送します。追加プロトコルを転送するには、このボックスにそれぞれの EtherType を追加する必要があります。このタイプは、4桁の 16進数を入力します。一般的な例として、AppleTalk（タイプ 809B）、Novell（タイプ 8138）、PPPoE（タイプ 8863 と 8864）が挙げられます。一般的な用途としては、接続されているネットワークで追加プロトコルを転送するために、RED インタフェース間のブリッジとすることが考えられます。

6.3 QoS

一般的に、*サービス品質*（QoS）とは、選択されたネットワークトラフィックにより良いサービスを提供する制御メカニズムを示し、特に、保証された帯域幅という点で優先することを意味します。Sophos UTMでは、優先トラフィックは、「*QoS*」タブで設定します。この設定では、ネットワークの2点間を通過する特定タイプの送信ネットワークトラフィックに対し、保証された帯域幅を確保できますが、一方で、受信トラフィックのシェーピングは SFQ（*確率的不偏キューイング*）あるいは RED（*ランダム初期検知*）などのさまざまなテクニックによって内部的に最適化されます。

6.3.1 ステータス

「*QoS > ステータス*」タブには、QoS を設定できるインタフェースがリストされます。デフォルトでは、QoS は各インタフェースに対して無効になっています。

インターフェースの QoS を設定するには、次の手順に従ってください。

1. **該当するインターフェースの「編集」ボタンをクリックします。**
   「*インターフェースの編集*」ダイアログボックスが開きます。

2. **次の設定を行います。**
ダウンリンク（キロビット/秒）、アップリンク（キロビット/秒）:ISP によって提供されるアップリンクおよびダウンリンク帯域幅（Kbps）を設定します。たとえば、アップリンクとダウンリンクの両方に 5Mビット/秒（Mbps）のインターネット接続を設定するには、「5120」と入力します。

帯域幅が変動する場合は、ISP が保証した最低の値を入力します。たとえば、アップリンクとダウンリンクの両方に 0.8Mビット/秒（Mbps）の変動のある 5Mビット/秒（Mbps）のインターネット接続を使用する場合は、4300Kビット/秒（Kbps）と入力します。利用できる帯域幅が一時的に設定した最低保証値より高くなると、ゲートウェイは新しい帯域幅を考慮して予想して、優先トラフィックの帯域幅のパーセンテージが同様に高くなるようにしますが、これは残念ながら、その反対には作用しません。

アップリンクを制限:このオプションを選択すると、QoS 機能は、設定されたダウンリンクとアップリンクの帯域幅を、このインタフェースを通過するトラフィックを優先順位付けするための計算ベースとして使用します。デフォルトでは「*アップリンクを制限*」オプションは選択されており、以下のインタフェースタイプに使用されます。

- イーサネットスタティックインタフェース（ゲートウェイとインターネット間にルータが配備され、ルータが提供する帯域幅がわかっているもの）
- 標準 VLAN インタフェース（ゲートウェイとインターネット間にルータが配備され、ルータが提供する帯域幅がわかっているもの）
- DSL（PPPoE）
- DSL（PPPoA）
- モデム（PPP）

トラフィックシェーピングの計算ベースがインタフェースの最大速度で決定されるインタフェースの「*アップリンクを制限*」チェックボックスからチェックを外します。ただし、これは以下のインタフェースタイプにのみ適用されます。

- イーサネットスタティックインタフェース（インターネットに直接接続）
- イーサネットVLANインタフェース（インターネットに直接接続）
- イーサネット DHCP

特定のアップリンク制限が指定されていないインタフェースでは、QoS 機能が全トラフィックを均等にシェーピングします。たとえば、イーサネット DHCP インタフェース上の VoIP トラフィックに 512Kビット/秒（Kbps）を設定した場合に、利用できる帯域幅が半分になったときは、256Kビット/秒がこのトラフィックに使用されます（比例シェーピングは、固定最大制限に依存するインタフェースと対照的に、双方向に機能することに注意してください）。

ダウンロードイコライザ:有効にすると、*確率的不偏キューイング*(SFQ)および*ランダム初期検知*(RED)キューアルゴリズムがネットワークの輻輳を回避します。設定したダウンリンク速度に達すると、ストリームを使用するほとんどのダウンリンクのパケットはドロップします。

アップロードオプティマイザ:有効にすると、送信 TCP 接続の確立(*SYN*フラグが設定されたTCPパケット)、TCP 接続の ACK(確認応答)パケット(*ACK*フラグが設定され、パケット長が 40～60バイトの TCP パケット)、および DNS ルックアップ(ポート 53上の UDP パケット)が自動的に優先されます。

3. **「*保存*」をクリックします。**
   設定が保存されます。
4. **QoS インタフェースを有効にします。**
   インタフェースのトグルスイッチをクリックします。トグルスイッチが緑色に変わります。

6.3.2 トラフィックセレクタ

トラフィックセレクタは、QoS が扱う特定タイプのネットワークトラフィックを記述した QoS の定義と見なすことができます。これらの定義は、後で帯域幅プール定義の中で使用されます。帯域幅プール定義では、帯域幅全体の制限や特定量の最低帯域幅の保証など、QoS によるこのトラフィックの取り扱い方法について定義できます。

トラフィックセレクタを作成するには、以下の手順に従います。

1. **「*トラフィックセレクタ*」タブで、「*新規トラフィックセレクタ*」をクリックします。**
   「*新規トラフィックセレクタの作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前:このトラフィックセレクタを説明する名前を入力します。

   セレクタタイプ:以下のタイプを定義できます。

   - **トラフィックセレクタ:**トラフィックセレクタを使用すると、トラフィックは 1つのサービスまたはサービスグループに基づいてシェーピングされます。
   - **アプリケーションセレクタ:**アプリケーションセレクタを使用すると、トラフィックはアプリケーションに基づいてシェーピングされます。つまり、使用するポートやサービスにかかわらず、トラフィックがそれぞれどのアプリケーションに属しているかに依存します。
   - **グループ:**複数のサービスおよびアプリケーションセレクタを 1つのトラフィックセレクタルールにまとめることができます。グループを定義するには、単体のセレクタをいくつか定義している必要があります。

送信元: QoSを有効にする送信元ネットワークを選択します。

サービス:*トラフィックセレクタのみ*で使用できます。QoSを有効にするネットワークサービスを選択します。事前に定義したさまざまなサービスやサービスグループから選択できます。たとえば、固定帯域幅をVoIP接続に予約する場合は、VoIP プロトコル(SIP および H.323)を選択します。

宛先: QoSを有効にする宛先ネットワークを選択します。

制御基準:*アプリケーションセレクタのみ*で使用できます。アプリケーションタイプに基づいてトラフィックをシェーピングするか、カテゴリに基づくダイナミックフィルタによってコントロールするかを選択します。

- **アプリケーション:**トラフィックは、アプリケーションに基づいてシェーピングされます。「*管理対象アプリケーション*」ボックスでアプリケーションを1つ以上選択します。
- **ダイナミックフィルタ:**トラフィックは、カテゴリに基づいてシェーピングされます。「*制御するカテゴリ*」ボックスでカテゴリを1つ以上選択します。

管理対象アプリケーション/カテゴリ:*アプリケーションセレクタのみ*で使用できます。「フォルダ」アイコンをクリックして、アプリケーション/カテゴリを選択します。ダイアログウィンドウが開きます。これについては、次のセクションで詳しく説明します。

生産性:*ダイナミックフィルタのみ*で使用きます。選択した生産性スコアが反映されます。

リスク:*ダイナミックフィルタのみ*で使用きます。選択したリスクスコアが反映されます。

注 – 一部のアプリケーションはシェーピングできません。これは、Sophos UTMの適切なオペレーションのために必要です。このようなアプリケーションは、「*アプリケーション選択*」ダイアログウィンドウのアプリケーションテーブルでチェックボックスがオフになっています。たとえば、*WebAdmin*、*Teredo*、*SixXs*(IPv6トラフィック用)、*Portal*(ユーザポータルのトラフィック用)などが該当します。ダイナミックフィルタを使用すると、これらのアプリケーションのシェーピングも自動的に制限されます。

コメント(任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**

TOS/DSCP(「*Traffic Selector*」のみで表示されます):特殊なケースでは、送信元、宛先、およびサービスだけでなく、IP ヘッダの TOS または DSCP フラグによって、QoS が処理するトラフィックを区別することが有益になります。

- **OFF**このデフォルトオプションでは、上で選択した送信元、サービス、および宛先と一致するすべてのトラフィックが QoS により処理されます。
- **TOS ビット:**QoS が処理するトラフィックを特定の TOS(サービスタイプ)ビット設定の IP パケットに制限する場合は、このオプションを選択します。TOS ビットの場合、以下の設定から選択できます。
  - 通常サービス
  - 金額的コストの最小化
  - 信頼性を最大化
  - スループットの最大化
  - 遅延の最小化
- **DSCP ビット:**QoS が処理するトラフィックを特定の DSCP(差別化サービスコードポイント)ビット設定の IP パケットに制限する場合は、このオプションを選択します。単一の「*DSCP 値*」(0～63 の整数)を指定するか、または「*DSCP クラス (DSCP Class)*」リストから事前に定義した値を選択できます(*BE default dscp (000000)*など)。

送受信データ量:接続によってそれまでに送信されたバイト量に基づいてトラフィックセレクタを一致させる場合は、このチェックボックスにチェックを入れます。この機能を使用すると、通常の HTTP トラフィックを制限することなく、大規模な HTTP アップロードの帯域幅を制限することなどができます。

- **送受信:**特定のトラフィック量を超過する接続のみのトラフィックセレクタを定義する場合は、ドロップダウンリストから「*下限*」を選択します。特定の量を下回る接続のトラフィックセレクタを定義する場合は、「*上限*」を選択します。
- **キロバイト:**トラフィック量のしきい値を入力します。

ヘルパー:データ通信に動的ポート範囲を使用するサービスもあります。各接続に対して、使用するポートをエンドポイント間で、コントロールチャネル経由でネゴシエートします。UTM では、コネクショントラッキングヘルパを使用して、コントロールチャネルをモニタリングし、どの動的ポートが使用されているかを判断します。動的ポート経由で送信されたトラフィックをトラフィックセレクタに含める場合は、上部の「*サービス*」ボックスで「*任意*」を選択し、「*ヘルパー*」ドロップダウンリストから適切なサービスを選択します。

4. **「*保存*」をクリックします。**
   新しいセレクタが「*トラフィックセレクタ*」リストに表示されます。

多くのトラフィックセレクタを定義した場合は、1つのトラフィックセレクタグループに複数のセレクタをまとめることで、より便利に使用することが可能になります。

このトラフィックセレクタまたはトラフィックセレクタグループは、それぞれの帯域幅プールで使用できます。これらのプールは「*帯域幅プール*」タブで定義できます。

「アプリケーションまたはカテゴリの選択」ダイアログウィンドウ

アプリケーションコントロールルールを作成する際は、「*管理するアプリケーション(カテゴリ)を 1つ以上選択してください*」というダイアログウィンドウからアプリケーションまたはアプリケーションカテゴリを選択する必要があります。

ダイアログウィンドウの下部に表示されるテーブルには、選択可能なアプリケーションまたは定義したカテゴリに属するアプリケーションが表示されます。デフォルトでは、すべてのアプリケーションが表示されます。

ダイアログウィンドウの上部には、テーブルに表示されるアプリケーション数を制限するための 3つの設定オプションがあります。

- **カテゴリ:**アプリケーションはカテゴリ別にグループ化されています。このリストには、利用可能なすべてのカテゴリが表示されます。デフォルトでは、すべてのカテゴリが選択されています。つまり、下部に表示されるテーブルには、利用可能なすべてのアプリケーションが表示されます。表示されるアプリケーションを特定のカテゴリに絞り込むには、クリックしてカテゴリリストを開き、1つ以上のカテゴリを選択します。
- **生産性:**アプリケーションは、生産性への影響(つまり生産性にこのアプリケーションが与える影響の度合い)によっても分類されています。例:一般的なビジネスソフトウェアの Salesforce のスコアは 5です。つまり、これを使用することで生産性が向上します。一方、オンラインゲームの Farmville のスコアは 1 で、これを使用すると生産性が低下します。ネットワークサービス DNS のスコアは 3 で、生産性への影響は中立的です。
- **リスク:**アプリケーションは、使用時のリスク(マルウェア、ウイルス感染、攻撃)によっても分類されています。数値が高いほど、リスクも高くなります。

ヒント – それぞれのアプリケーションには情報アイコンがあり、クリックすると各アプリケーションの説明が表示されます。テーブルヘッダのフィルタフィールドを使用して、テーブル内を検索することができます。

次に、「*新規トラフィックセレクタの作成*」ダイアログボックスで選択したコントロールのタイプに応じて、以下を行います。

- ダイナミックフィルタで管理する場合:「*適用*」をクリックして、選択したアプリケーションをルールに適用します。

- アプリケーションで管理する場合:テーブルで、アプリケーションの前にあるチェックボックスをクリックし、管理対象のアプリケーションを選択します。「*適用*」をクリックして、選択したアプリケーションをルールに適用します。

「*適用*」をクリックするとダイアログウィンドウが閉じ、トラフィックセレクタルールの設定の編集を続けることができます。

6.3.3 帯域幅プール

「*QoS > 帯域幅プール*」タブで、帯域幅を管理するための帯域幅プールを定義して管理できます。帯域幅プールでは、特定の送信タイプに対して保障帯域幅を予約します。任意で、最大帯域幅を指定してこれを制限することもできます。

帯域幅プールを作成するには、以下の手順に従います。

1. **「*帯域幅プール*」タブで、インタフェースを選択します。**
   ドロップダウンリストから、帯域幅プールを作成するインタフェースを選択します。
2. **「*新規帯域幅プール*」をクリックします。**
   「*新規帯域幅プールの作成*」ダイアログボックスが開きます。
3. **次の設定を行います。**
   名前:この帯域幅プールを説明する名前を入力します。

   位置:位置番号。これによって帯域幅プールの優先順位が定義されます。番号が小さいほど優先順位が高くなります。帯域幅プールは昇順に照合されます。ある帯域幅プールが一致すると、それ以降、それより大きい番号の帯域幅プールは評価されません。より具体的な帯域幅プールをリストの上部に配置して、曖昧な帯域幅プールが最後に照合されるようにします。たとえば、一般的な Web トラフィック(HTTP)と特定ホストへの Web トラフィックにトラフィックセレクタを設定した場合は、帯域幅プールリストの最上部に後者のトラフィックセレクタを使用する帯域幅プールを配置します(つまり、位置 1 をそれに選択します)。

   帯域幅:この帯域幅プール用に予約するアップリンク帯域幅をキロビット単位で入力します。たとえば、特定タイプのトラフィックに 1M ビット/秒(Mbps)を予約する場合は、`1024` と入力します。

   注 – 帯域幅プールに割り当てられるのは、利用可能な全帯域幅の 90 %までです。ゲートウェイは常に帯域幅の 10 %をいわゆるシェーピングされていないトラフィック用に予約します。上記の例で言えば、アップリンクのインターネット接続が 5M ビット/秒(Mbps)で、VoIP

トラフィックにできるだけ多くの帯域幅を割り当てたい場合は、最大 4608K ビット/秒 (Kbps) を入力できます。

帯域幅の上限を指定する:上記の「*帯域幅*」フィールドに入力した値は、特定の種類のトラフィック用に予約される保証された帯域幅を示します。しかし、帯域幅プールは通常、可能であれば、そのトラフィック用により多くの帯域幅を割り当てます。特定のトラフィックが一定量以上の帯域幅を使用しないようにしたい場合は、このオプションを選択して、この帯域幅プールによって使用される帯域幅の割り当てを上限値に制限します。

トラフィックセレクタ:この帯域幅プールに使用するトラフィックセレクタを選択します。

コメント (任意):説明などの情報を追加します。

4. **「*保存*」をクリックします。**
   新しい帯域幅プールが「*帯域幅プール* 」リストに表示されます。
5. **ルールを有効にします。**
   新しいルールはデフォルトで無効になっています (トグルスイッチはグレー表示)。ルールを有効にするには、トグルスイッチをクリックします。

   これでルールが有効になります (トグルスイッチは緑色)。

帯域幅プールを編集または削除するには、対応するボタンをクリックします。

6.3.4 ダウンロード帯域幅調整

「*QoS > ダウンロード帯域幅調整*」タブで、受信トラフィックの帯域幅を調整するためのルールを設定・管理できます。設定したしきい値より速い速度でパケットが送られてくる場合、過剰なパケットは、ファイアウォールルールのログファイルに記録されることなく、直ちに破棄されます。TCP 輻輳制御避方法により、破棄されたパケットを送信した送信者は、送信する頻度を減らす必要があります。

ダウンロード帯域幅調整ルールを作成するには、以下の手順に従います。

1. **「*ダウンロード帯域幅調整*」タブで、インタフェースを選択します。**
   ドロップダウンリストから、ダウンロード帯域幅調整を作成するインタフェースを選択します。
2. **「*新規ダウンロード帯域幅調整ルール*」をクリックします。**
   「*新規ダウンロード帯域幅調整ルール*」ダイアログボックスが開きます。
3. **次の設定を行います。**
   名前:このダウンロード帯域幅調整ルールを説明する名前を入力してください。

優先順位:優先順位番号。これによってルールの優先順位が定義されます。番号が小さいほど優先順位が高くなります。ルールは昇順に照合されます。あるルールが一致すると、それ以降、それより大きい番号のルールは評価されません。より具体的な帯域幅ルールをリストの上部に配置して、曖昧な帯域幅ルールが最後に照合されるようにします。

制限値(キロビット/秒):指定したトラフィックの上限(単位:キロビット)。たとえば、特定タイプのトラフィックの帯域幅を1Mビット/秒(Mbps)に制限する場合は、1024と入力します。

制限:上で指定した制限を適用するトラフィックの送信元や宛先:

- **共有:**既存の接続すべてに、上限を均等に分散します。つまり、このルールで指定されるトラフィック全体のダウンロード帯域幅は、指定した値に制限されます。
- **各送信元アドレス:**送信元アドレスごとに、この上限値が適用されます。
- **各宛先アドレス:**宛先アドレスごとに、この上限値が適用されます。
- **各送信元/宛先:**双方向アドレスペアごとに、この上限値が適用されます。

トラフィックセレクタ:ダウンロード帯域幅を調整するトラフィックセレクタを選択します。選択したトラフィックセレクタ間で、上限値が分散されます。

コメント(任意):説明などの情報を追加します。

4. **「*保存*」をクリックします。**
   新しいダウンロード帯域幅調整ルールが、「*ダウンロード帯域幅調整*」リストに表示されます。
5. **ルールを有効にします。**
   新しいルールはデフォルトで無効になっています(トグルスイッチはグレー表示)。ルールを有効にするには、トグルスイッチをクリックします。

   これでルールが有効になります(トグルスイッチは緑色)。

ルールを編集または削除するには、対応するボタンをクリックします。

6.3.5 詳細

カプセル化の後も分類を維持する

カプセル化後にパケットが他のトラフィックセレクタが一致しない場合に、元のサービスのトラフィックセレクタと引き続き一致することを確認する場合は、このチェックボックスにチェックを入れます。

トラフィックセレクタへのカプセル化されたIPパケットの割り当ては、次のように機能します。

1. 元の IP パケットを与えられた順序で既存のトラフィックセレクタと比較します。パケットが最初に一致するトラフィックセレクタに割り当てられます(内部 -> HTTP -> 任意など)。
2. IP パケットがカプセル化され、サービスが変更されます(IPsec などへ)。
3. カプセル化したパケットを与えられた順序で既存のトラフィックセレクタと比較します。パケットが最初に一致するトラフィックセレクタに割り当てられます(内部 -> IPsec -> 任意など)。
4. 一致するトラフィックセレクタがない場合の割り当ては、「*カプセル化後もクラシフィケーションを保持*」オプションに依存します。
   - このオプションが選択されている場合、カプセル化したパケットが手順1で検出したトラフィックセレクタに割り当てられます。
   - このオプションが選択されていない場合、カプセル化したパケットはトラフィックセレクタに割り当てられないため、帯域幅プールの一部にすることができません。

Explicit Congestion Notification(ECN) サポート

ECN(明示的な輻輳通知)とはインターネットプロトコルの拡張であり、ネットワーク輻輳のエンドツーエンドな通知をパケットのドロップなしで許可します。ECN は、接続の両エンドポイントの間で使用のネゴシエートが成功している場合にのみ機能します。このチェックボックスにチェックを入れると、UTMは、ECN 使用の意向を伝える情報を送信します。他のエンドポイントが合意すると、エンドポイントが ECN 情報を交換します。下位のネットワークと関与するルータも ECN をサポートしている必要があります。

6.4 アップリンクモニタリング

「*インタフェース & ルーティング > アップリンクモニタリング*」メニューでは、アップリンク接続をモニタリング(監視)し、接続ステータスが変化したときに自動的に適用するアクションを定義することができます。

たとえば、別のリンクを使用してバックアップ VPN トンネルを自動的にオンにしたり、エイリアス IP アドレスを無効にしてモニタリングサービスをトリガすることができます。

6.4.1 グローバル

「*アップリンクモニタリング > グローバル*」タブで、アップリンクのモニタリングを有効または無効にできます。

アップリンクモニタリングを有効にするには、トグルスイッチをクリックします。
トグルスイッチが緑色に変わります。

アップリンクモニタリングが有効の場合、「*アップリンクステータス*」セクションに、現在のアップリンクインターフェースおよびそのステータスが表示されます。

- *ONLINE:*アップリンク接続が確立し、機能しています。
- *OFFLINE:*モニタリングの結果、アップリンク接続はダウンしています。
- *DOWN:*アップリンクインターフェースが管理的な理由で無効化されている、または、動的インターフェースの場合、リモート PPP またはDHCP サーバに接続できません。
- *STANDBY:*「*インターフェース > アップリンクバランス*」タブで「スタンバイインタフェース」として指定されているインターフェースで、現在使用されていません。

注 – アップリンクバランスが有効になっている場合、アップリンクモニタリングが無効になっていても、アップリンクは常に監視されます。したがって、アップリンクモニタリングが無効になっていても、アップリンクバランスが有効になっている限り、このページにアップリンクインターフェースが表示されます。この場合、モニタリング設定は、「*インターフェース > アップリンクバランス*」タブで変更できます。

6.4.2 アクション

「*インタフェース & ルーティング (Interfaces & Routing) > アップリンクモニタリング > アクション*」タブで、アップリンクの接続ステータスが変更になった場合に自動的に適用するアクションを定義できます。たとえば、アップリンク接続がダウンした場合は追加アドレスを無効にすることができます。

新しいアクションを作成するには、以下の手順に従います。

1. **「アクション」タブで、「*新規アクション*」をクリックします。**
   「*アップリンクオフライン時の新規アクションの作成*」ダイアログウィンドウが開きます。
2. **次の設定を行います。**
   名前:アクションを説明する名前を入力します。

   タイプ:アクションを定義する接続タイプを選択します。

   - **IPsecトンネル:**IPsecトンネルに対するアクションを定義する場合は、ドロップダウンリストからこのオプションを選択します。
   - **追加アドレス:**追加アドレスに対するアクションを定義する場合は、ドロップダウンリストからこのオプションを選択します。

IPsecトンネル:(「*IPsecトンネル*」タイプのみに利用可。)IPsecトンネルを定義している場合は、ここでそれらのいずれかを選択できます。IPsecトンネルに関する詳細は、「*リモートアクセス > IPsec*」の章を参照してください。

追加アドレス:(「*追加アドレス*」タイプのみに利用可。)追加アドレスを定義している場合は、ここでそれらのいずれかを選択できます。追加アドレスに関する詳細は、「*インタフェース & ルーティング > インタフェース > 追加アドレス*」の章を参照してください。

アクション:ここで「*有効*」または「*無効*」のいずれかを選択できます。つまり、アップリンクが中断した場合は、上記で選択したIPsecトンネルや追加アドレスが有効または無効になるように設定します。

コメント(任意):説明などの情報を追加します。

3. **「保存」をクリックします。**
   アクションは保存され、アップリンクの接続が中断すると適用されます。

アクションを編集または削除するには、対応するボタンをクリックします。

6.4.3 詳細

「*アップリンクモニタリング > 詳細*」タブで、アップリンク接続の自動モニタリングを無効にしたり、モニタリング(監視)に使用する1つ以上のホストを定義できます。

デフォルトでは、インタフェース障害の可能性を検出するために「*自動モニタリング*」が有効になっています。つまり、すべてのアップリンク バランシング インタフェースからインターネット上の特定のホストに15秒間隔で接続することにより、それらのインタフェースの状態(健全性)がモニタリングされます。デフォルトでは、ホストのモニタリングは、1つのルートDNSサーバまでのルート上にある、pingを許可する3番目のホップです。なお、ユーザはサーバプールをモニタリングするためのホストを自分で定義することができます。これらのホストには、ping以外の別のサービスを選択し、モニタリング間隔とタイムアウトを変更できます。

各モニタリングホストには、一定期間接続を試み、いずれにも到達できない場合は、アップリンク接続はダウンしていると判断されます。その後、「*アクション*」タブで定義したアクションが実行されます。

注 – 同じモニタリング設定が、アップリンクモニタリング(*アップリンクモニタリング > 詳細*)とアップリンクバランシング(*インターフェース > アップリンクバランシング*)に対して使用されます。

モニタリングにお客様のホストを使用するには、以下の手順に従います。

1. **「*自動モニタリング*」チェックボックスのチェックを外します。**
「*モニタリングホスト*」ボックスが編集可能になります。

2. **モニタリングホストを追加します。**
任意のホストを使用する代わりに、モニタリングに使用するホストを 1つ以上追加します。複数のホストでインタフェースをモニタリングする場合、定義された時間内にすべてのモニタリングホストが応答しない場合にのみ、インタフェースがデッド（dead）とみなされます。

注 – 選択したホストがインタフェースに関連付けられている場合は、このインタフェースのモニタリングのみに使用されます。ホストがインタフェースに関連付けられていない場合は、すべてのインタフェースのモニタリングに使用されます。選択したホストによりカバーされていないインタフェースは、自動モニタリングによりモニタリングされます。

ボックスのヘッダにある「モニタリング設定」アイコンをクリックすると、モニタリングの詳細を設定できます。

モニタリングタイプ:モニタリング用のサービスプロトコルを選択します。モニタリング用に「*TCP*」(TCP 接続の確立)、「*UDP*」(UDP 接続の確立)、「*Ping*」(ICMP Ping)、「*HTTP ホスト*」(HTTP 要求)、または「*HTTPS ホスト*」(HTTPS 要求）のいずれかを選択します。「*UDP*」を使用する場合、ping 要求が最初に送信され、成功した場合は、続いてペイロード 0 の UDP パケットが送信されます。ping が成功しなかった場合や、ICMP ポートに到達できない場合、この接続はダウンしているとみなされます。

ポート（「*TCP*」および「*UDP*」のモニタリングタイプ選択時のみ):要求の送信先のポート番号。

URL（任意。「*HTTP/S ホスト*」のモニタリングタイプ選択時のみ):要求する URL。URL にポート情報を追加することで、デフォルトのポート 80 または 443 以外のポートを使用できます（例: `http://example.domain:8080/index.html`)。URL を指定しない場合は、ルートディレクトリが要求されます。

間隔:ホストをチェックする間隔を秒単位で入力します。

タイムアウト:モニタリングホストが応答を送信する最大時間を秒単位で入力します。インタフェースのすべてのモニタリングホストがこの時間内に応答しない場合、インタフェースがデッド（dead）とみなされます。

3. **「*適用*」をクリックします。**
設定が保存されます。

6.5 IPv6

Sophos UTMでは、バージョン 8 より、IPv4 の後継である IPv6 をサポートしています。

UTMの以下の機能では、IPv6 が完全にまたは部分的にサポートされます。

- WebAdmin およびユーザポータルへのアクセス
- SSH
- NTP
- SNMP
- SLAAC（ステートレスアドレス自動設定）および DHCPv6 クライアントはすべての動的インタフェースタイプをサポートしています。
- DNS
- DHCP サーバ
- BGP
- OSPF
- IPS
- ファイアウォール
- NAT
- ICMP
- サーバロードバランシング
- Web フィルタ
- Web アプリケーション ファイアウォール
- SMTP
- IPsec（サイト間のみ）
- Syslog サーバ

6.5.1 グローバル

「*IPv6 > グローバル*」タブでは、Sophos UTMの IPv6 サポートを有効にすることができます。さらに、これを有効にすると、IPv6 の情報（ステータス情報やプレフィックス委託など）がここに表示されます。

IPv6 サポートはデフォルトでは無効になっています。IPv6 を有効にするには、次の手順に従います。

1. **「*グローバル*」タブで、IPv6 を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色に変わります。以前に IPv6 を有効化または設定したことがない場合は、「*接続*」エリアに「*なし*」と表示されます。

IPv6 を有効にすると、複数のネットワークや、WebAdmin で IPv6 を明示的に参照しているその他のオブジェクト定義が表示されます。これらは、IPv4 オブジェクトと同様に使用することができます。

注 – IPv6 を有効にすると、ネットワークオブジェクトなどのアイコンに、該当オブジェクトが IPv6 オブジェクトか IPv4 オブジェクトか（あるいはその両方か）を示すマークが追加で表示されます。

6.5.2 プレフィックス広告

「*IPv6 > プレフィックス通知*」タブでは、Sophos UTMを設定して、クライアントに IPv6 アドレスプレフィックスを割り当てて、クライアントが自力で IPv6 アドレスを選択できるように設定することができます。プレフィックス通知（またはルータ通知）とは、IPv6 の機能の 1つであり、ルータ（この場合UTM）が IPv4 における DHCP サーバと同じように機能します。ただし、ルータはクライアントにIP を直接割り当てません。代わりに、IPv6 ネットワーク内のクライアントは、ルータとのプライマリ通信のためにいわゆるリンクローカルアドレスを自らに割り当てます。続いて、ルータがクライアントにネットワークセグメントのプレフィックスを伝えます。その後、クライアントはプレフィックスと自らの MAC アドレスから成る IP アドレスを生成します。

新しいプレフィックスを作成するには、次の手順に従います。

1. **「*プレフィックス通知*」タブで、「*新規プレフィックス*」をクリックします。**
   「*新規プレフィックスの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   インタフェース:64ビットのネットマスクが設定された IPv6 アドレスを持つインタフェースを選択します。

DNS サーバ 1/2(任意):DNS サーバの IPv6 アドレス。

ドメイン(任意):クライアントに送信されるドメイン名を入力します(例: `intranet.example.com`)。

有効期間:プレフィックスが有効な期間。デフォルトは 30日間です。

推奨期間:この期間を超過すると、推奨されるライフタイムがまだ満了していない他のプレフィックスがクライアントに選択されます。デフォルトは 7日間です。

他の設定(任意):このオプションはデフォルトで選択されています。これにより、所与のプレフィックスに対して所与の DNS サーバとドメイン名が DHCPv6 経由で追加でアナウンスされます。現時点では、プレフィックス通知から DNS 情報をフェッチできるクライアントは少ないため、この機能が役に立ちます(RFC 5006/ RFC 6106)。この DHCPv6 設定は非表示であり、DHCP 設定メニューでの表示や編集はできません。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しいプレフィックス設定が「*プレフィックス通知*」リストに表示されます。

6.5.3 再割り当て

「*IPv6 > 再割り当て*」タブで、プレフィックスが変更された場合に、UTM で管理される IPv6 アドレスが自動的に再割り当てされるよう設定することができます。また、手動で IPv6 を再割り当てすることもできます。

変更される IPv6 アドレスは次のとおりです。

- ホスト、ネットワーク、および範囲の定義
- プライマリおよびセカンダリ インターフェース アドレス
- DHCPv6 サーバ範囲とマッピング
- DNS マッピング

トンネルブローカで提供される IPv6 プレフィックスは、再割り当てされません。

自動 IPv6 再割り当て

デフォルトで、UTM で管理している IPv6 アドレスは、IPv6 プレフィックスが変更した際、自動的に再割り当てされます。プレフィックスの変更は、DHCPv6 プレフィックス委託経由で ISP によって実行されます。再割り当てを無効にするには、このチェックボックスを選択から外して、「*適用*」をクリックします。

手動 IPv6 再割り当て

UTM で管理される特定の IPv6 アドレスを手動で再割り当てすることができます。これは ISP を変更し、新しいプロバイダが、IPv6 プレフィックスを DHCPv6 経由で自動的に割り当てるのでなく、静的に割り当てた場合などに便利です。

1. **再割り当てする IPv6 アドレスのプレフィックスを指定します。**
   プレフィックスを「*古いプレフィックス*」フィールドに入力します。
2. **新しいプレフィックスを指定します。**
   プレフィックスを「*新規プレフィックス*」フィールドに入力します。
3. **「*適用*」をクリックします。**

   指定したプレフィックスのある IPv6 アドレスはすべて、新しいプレフィックスを使用して再割り当てされます。

6.5.4 6to4

「*IPv6 > 6to4*」タブでは、既存の IPv4 ネットワーク上で IPv6 アドレスを自動的にトンネリングするようにSophos UTMを設定することができます。6to4 を使用すると、各 IPv4 アドレスに、マッピング先の IPv6 ネットワークから `/48` プレフィックスが付加されます。生成される IPv6 アドレスは、プレフィックス `2002` と16進表記の IPv4 アドレスから構成されます。

注 – 「*6to4*」を有効にするか「*トンネルブローカ*」を使用するかのいずれかを選択できます。

特定のインタフェースのIPアドレストンネリングを有効にするには、次の手順に従います。

1. **「*6to4*」タブで 6to4 を有効化します。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*6to4*」エリアと「*詳細*」エリアが編集可能になります。
2. **インタフェースを選択します。**
   「*インタフェース*」ドロップダウンリストから、パブリック IPv6 アドレスが設定されているインタフェースを選択します。
3. **「*適用*」をクリックします。**
   設定が保存されます。インタフェースのステータスが「*グローバル*」タブに表示されます。

詳細

「*サーバアドレス*」を変更して、別の 6to4 リレーサーバを使用することができます。

設定を保存するには「*適用*」をクリックします。

6.5.5 トンネルブローカー

「*IPv6 > トンネルブローカー*」タブでは、トンネルブローカーの使用を有効にすることができます。トンネルブローカーは一部の ISP が提供するサービスであり、これを利用すると IPv6 アドレスを使用してインターネットにアクセスできます。

注 – 「*6to4*」を有効にするか「*トンネルブローカー*」を使用するかのいずれかを選択できます。

Sophos UTM は、次のトンネルブローカーをサポートします。

- Teredo（匿名のみ）
- Freenet6（GoGo6）（匿名またはユーザアカウント使用）
- SixXS（ユーザアカウントが必要）

トンネルブローカーを使用するには、次の手順に従います。

1. **「*トンネルブローカー*」タブで、トンネルブローカーの使用を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、「*トンネルブローカー*」エリアと「*詳細*」エリアが編集可能になります。Teredo の匿名認証を使用すると、トンネルブローカーはすぐに有効になります。接続ステータスが「*グローバル*」タブに表示されます。

トンネルブローカー

デフォルトのトンネルブローカー設定を変更できます。

認証:ドロップダウンリストから認証方法を選択します。

- **匿名:**この方法を使用すると、各ブローカーにユーザアカウントを指定する必要はありません。割り当てられる IP アドレスは一時的なものです。
- **ユーザ:**各ブローカーに登録して、ユーザアカウントを取得する必要があります。

ブローカー:ドロップダウンリストから他のブローカーを選択できます。

ユーザ名（*ユーザのみで使用可*）:各ブローカにユーザ名を指定します。

パスワード（*ユーザのみで使用可*）:ユーザ名のパスワードを入力します。

設定を保存するには「*適用*」をクリックします。

詳細

ここでは、選択したトンネルブローカーに対して他のサーバアドレスを指定できます。

設定を保存するには「*適用*」をクリックします。

6.6 スタティックルーティング

ネットワークに接続されたすべてのコンピュータは、ルーティングテーブルを使用して、発信したデータパケットを宛先に届くように送信するためのパスを決定します。たとえば、ルーティングテーブルには、宛先アドレスがローカルネットワーク上にあるか、またはデータパケットをルータに転送するべきかどうか、といった情報が含まれています。ルータを使用する場合は、テーブルには、どのルータをどのネットワークに使用するかという情報が含まれます。

Sophos UTMのルーティングテーブルには、標準スタティックルートとポリシールートという2種類のルートを追加できます。スタティックルートでは、ルーティングターゲットはパケットの宛先アドレスだけで決定されます。ポリシールートでは、送信元インタフェース、送信元アドレス、サービス、あるいは宛先アドレスに基づいてルーティングを決定できます。

注 – UTM のインタフェースに接続されたネットワークに対して、追加ルートを設定する必要はありません。また、デフォルトルートも設定する必要はありません。これらのルートはシステムが自動的に追加します。

6.6.1 標準スタティックルート

システムに直接接続されたネットワークについては、システムがルーティングエントリをルーティングテーブルに自動的に挿入します。特定ネットワーク経由でアクセスする追加ルータを使用する場合は、エントリを手動で入力する必要があります。直接接続されていないネットワークへのルートで、コマンドまたは設定ファイルを使ってルーティングテーブルに挿入されるものをスタティックルートと呼んでいます。

標準スタティックルートを追加するには、以下の手順に従います。

1. **「*標準スタティックルート*」タブで、「*新規スタティックルート*」をクリックします。**
   「*新規スタティックルートを作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   ルートタイプ:次のルートタイプを使用できます。

- **インタフェースルート:**パケットは特定のインタフェース上で送信されます。これは 2つの状況で役立ちます。1つ目は、ゲートウェイの IP アドレスが不明になるダイナミック(動的)インタフェース(PPP)上でルーティングする場合です。2番目は、直接接続されたネットワークの外側にゲートウェイがあるデフォルトルートを定義する場合です。
- **ゲートウェイルート:**パケットは特定のホスト(ゲートウェイ)へ送信されます。
- **ブラックホールルート:**パケットは確認なしで廃棄されます。これは OSPF または他のダイナミックアダプティブ(動的適応型の)ルーティングプロトコルでルーティングループやルートフラッピングなどを回避する場合に役に立ちます。

ネットワーク:UTM がインターセプトするデータパケットの宛先ネットワークを選択します。

インタフェース:データパケットが UTM を離れるインタフェースを選択します(ルートタイプとして「*インタフェースルート*」を選択した場合のみ使用可)。

ゲートウェイ:UTM がデータパケットを転送するゲートウェイ/ルータを選択します(ルートタイプに「*ゲートウェイルート*」を選択した場合のみ使用可)。

コメント(任意):説明などの情報を追加します。

3. **オプションで、次の詳細設定を行います。**
   メトリック:0～4294967295 の整数でメトリック値を指定します。デフォルトは 5です。メトリック値は同じ宛先へのルートを区別して優先するために使用されます。低いメトリック値の方が、高いメトリック値よりも優先されます。IPsec ルートのメトリックは自動的に 0 に設定されます。
4. **「*保存*」をクリックします。**
   新しいルートが「*標準スタティックルート*」リストに表示されます。
5. **ルートを有効にします。**
   ルートを有効にするには、トグルスイッチをクリックします。

ルートを編集または削除するには、対応するボタンをクリックします。

6.6.2 ポリシールート

ルータがデータパケットを受信すると、通常はパケットの宛先アドレスに基づいて転送先を決定し、この宛先アドレスを使用してルーティングテーブルのエントリが検索されます。ただし、他の基準に基づいてパケットを転送することが必要な場合もあります。ポリシーベースのルーティングでは、お客様のポリシーに従ってデータパケットをフォワーディング(転送)またはルーティングできます。

ポリシールートを追加するには、以下の手順に従います。

1. **「*ポリシールート*」タブで、「*新規 IPsec ポリシー*」をクリックします。**
「*新規ポリシールートを作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
位置:位置番号。これによってポリシールートの優先順位が定義されます。番号が小さいほど優先順位が高くなります。ルートは昇順に照合されます。あるルートが一致すると、それ以降、それより大きい番号のルートは評価されません。

ルートタイプ:次のルートタイプを使用できます。

- **インタフェースルート:**パケットは特定のインタフェース上で送信されます。これは 2つの状況で役立ちます。1つ目は、ゲートウェイの IP アドレスが不明になるダイナミック(動的)インタフェース(PPP)上でルーティングする場合です。2番目は、直接接続されたネットワークの外側にゲートウェイがあるデフォルトルートを定義する場合です。
- **ゲートウェイルート:**パケットは特定のホスト(ゲートウェイ)へ送信されます。

送信元インタフェース:ルーティングされるデータパケットが到着したインタフェース。「すべて」を設定すると、すべてのインタフェースが該当することになります。

送信元ネットワーク:ルーティングされるデータパケットの送信元ネットワーク。「すべて」を設定すると、すべてのネットワークが該当することになります。

サービス:ルーティングされるデータパケットに一致するサービス定義。ドロップダウンリストには、定義済みのサービスとお客様が定義されたサービスがすべて含まれます。これらのサービスにより、どのようなトラフィックを処理するかを精密に指定できます。「すべて」を設定すると、プロトコル、送信元、および宛先ポートのあらゆる組み合わせに一致します。

宛先ネットワーク:ルーティングされるデータパケットの宛先ネットワーク。「すべて」を設定すると、すべてのネットワークが該当することになります。

ターゲットインタフェース:データパケットの送信先インタフェース(ルートタイプとして「*インタフェースルート*」を選択したときのみ使用可)。

ゲートウェイ:ゲートウェイがデータパケットを転送するゲートウェイ/ルータを選択します(ルートタイプに「*ゲートウェイルート*」を選択した場合のみ使用可)。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
新しいポリシーが「*ポリシールート*」リストに表示されます。

4. **ルートを有効にします。**
ルートを有効にするには、トグルスイッチをクリックします。

ルートを編集または削除するには、対応するボタンをクリックします。

6.7 OSPF

OSPF(Open Shortest Path First)プロトコルは、リンクステート型の階層ルーティングプロトコルであり、大規模な自律システム(AS)ネットワーク内で主に使用されます。Sophos UTMは OSPF バージョン 2をサポートしています。他のルーティングプロトコルと比べ、OSPF はルーティングメトリックとしてコストを使用しています。OSPF 対応インタフェースのコストは、特定のインタフェース経由でパケットを送信するときに必要なオーバーヘッドを示します。インタフェースのコストは、そのインタフェースの帯域幅に反比例します。そのため、帯域幅が大きいと、コストが小さくなります。たとえば、10 Mbps のイーサネット回線より 56 Kbps のシリアル回線の方がオーバーヘッドが増え(コストが高くなり)、遅延時間が長くなります。

接続されたネットワークのコストの計算方法は、OSPF 仕様には指定されておらず、ベンダーに任されています。そのため、独自の計算式を定義することができます。ただし、コストがすでに定義されている他のネットワークとOSPF ネットワークが隣接している場合、同じ計算ベースを適用することをお勧めします。

デフォルトでは、インタフェースのコストは帯域幅に基づいて計算されます。たとえば、Cisco の場合、10^8 をインタフェースの帯域幅(bps)で割ってコストを計算しています。この計算式を使用すると、10 Mbps のイーサネット回線を経由する場合のコストは $10^8/10000000 = 10$ となります。一方、1.544 Mbps の回線(T1)では、$10^8/1544000 = 64$ となります(コストの計算では、小数点以下を切り捨てます)。

6.7.1 グローバル

「*インタフェース & ルーティング > ダイナミックルーティング (OSPF) > グローバル*」タブでは、OSPF の基本設定を行うことができます。OSPF 機能を有効にする前に、OSPF エリアを1つ以上設定しておく必要があります(*エリア*」タブ)。

警告 – Sophos UTMの OSPF 機能を設定するためには、OSPF プロトコルを熟知している技術的に熟練した経験豊富な管理者が必要です。ここでの設定オプションについての解説は、OSPF プロトコルについて完全に理解するために十分であるとは言えません。そのため、この機能は慎重に使用することをお勧めします。設定を誤ると、ネットワークが動作不可能になる場合があります。

OSPF を設定するには、次の手順に従ってください。

1. **「*エリア*」タブで、OSPF エリアを 1つ以上作成します。**
2. **「*グローバル*」タブで、OSPF を有効化します。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*ルータ*」エリアが編集可能になります。
3. **ルータ ID を入力します。**
   Sophos UTMデバイスを他の OSPF ルータから識別するための独自のルータ ID を入力します。
4. **「*適用*」をクリックします。**
   設定が保存されます。

OSPF を無効にするには、トグルスイッチをクリックします。

6.7.2 エリア

OSPF ネットワークは、複数のエリアに分割されます。エリアとは、ネットワークの残りの部分のために情報をひとまとめにできるルータの論理グループです。エリアの識別名は、10進ドット表記の32ビット ID であり、IP アドレスの表記法と似ています。

OSPF エリアは全部で 6種類あります。

- **バックボーン:**ID が 0(または `0.0.0.0`)のエリアは OSPF ネットワークバックボーンに予約されており、OSPF ネットワークの中核となります。他のすべてのエリアがこのエリアに接続されます。
- **標準:**標準エリアは、1(または `0.0.0.1`)～ 4,294,967,295(または `255.255.255.255`)という一意の ID 範囲を持ちます。ノーマルエリアは、ABR (*エリア境界ルータ*)を介して外部ルートを双方向的にフラッディングして処理します。外部ルートとは、他のルーティングプロトコルから OSPF 内に配布されたルートとして定義されます。
- **スタブ:**通常、スタブエリアは外部ネットワークと直接接続されません。外部ネットワークへのすべてのトラフィックは ABR (*エリア境界ルータ*)を介してルーティングする必要があるため、Stub エリアに外部ルートをインジェクトする必要はありません。そのため、スタブエリアは外部ネットワークにトラフィックを送信する外部ルートにとってデフォルトルートの代わりとなります。
- **スタブサマリなし:**「*スタブサマリなし*」エリアや「*完全なスタブエリア*」は、スタブエリアと似ていますが、いわゆるサマリルートは許可されていません。つまり、タイプ 3 のサマリ リンクステートアドバタイズメント(LSA)がエリアに入ってこないようにします。

- **NSSA:**NSSA (not-so-stubby area) は、スタブエリアとは異なり、外部接続をサポートできます。NSSA はバーチャルリンクに対応していません。
- **NSSA サマリなし:**「*NSSA サマリなし*」は NSSA と似ていますが、このエリアではいわゆるサマリルートは許可されていません。つまり、タイプ 3 のサマリリンクステートアドバタイズメント (LSA) がエリアに入ってこないようにします。

OSPF エリアを作成するには、次の手順に従います。

1. **「エリア」タブで「*新規 OSPF エリア*」をクリックします。**
   「*新規 OSPF エリアの作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前:エリアを説明する名前を入力してください。

   エリア ID:エリアの ID を 10進ドット表記で入力します (たとえば通常エリアは `0.0.0.1`、バックボーンエリアは `0.0.0.0` など)。

   エリアタイプ:前述のエリアタイプを選択し、該当するエリアに割り当てられるネットワークの特徴を指定します。

   認証タイプ:エリア内のインタフェースを介して送受信されるすべての OSPF パケットに対して使用する認証タイプを選択します。次の認証タイプを使用できます。

   - **MD5:**選択すると、MD5 認証が有効になります。MD5 (Message-Digest algorithm 5) とは、128ビットのハッシュ値を使用する一般的な暗号ハッシュ関数です。
   - **平文:**選択すると、平文認証が有効になります。パスワードはネットワーク上を平文の形で伝送されます。
   - **OFF:**選択すると、認証が無効になります。

   接続経由インタフェース:OSPF 対応インタフェースを選択します。ここで OSPF 対応インタフェースを指定するためには、事前に「*インタフェース*」タブでこのインタフェースを作成しておく必要があります。

   バーチャルリンクを使用:OSPF *自律システム* (AS) 内のすべてのエリアは、バックボーンエリア (エリア 0) に物理的に接続されている必要があります。物理的な接続が不可能な場合には、バーチャルリンクを使用して、非バックボーンエリアを介してバックボーンに接続できます。「*仮想リンクの接続*」ボックスに、バーチャルリンクのネイバーに関連付けられたルータ ID を 10進ドット表記で入力します (`10.0.0.8` など)。

   コスト:このエリアでデータパケットを送受信するコスト。有効な値は 1～65535 の範囲内です。

   コメント (任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しいエリア定義が「*エリア*」タブに表示されます。

OSPF エリアを編集または削除するには、対応するボタンをクリックします。

ライブログを開く:OSPF ライブログには、OSPF インタフェースでのすべてのアクティビティが記録されます。ボタンをクリックして、新しいウィンドウでライブログを開きます。

6.7.3 インタフェース

「*インタフェース & ルーティング > ダイナミックルーティング (OSPF) > インタフェース*」タブでは、OSPF エリア内で使用するインタフェースの定義を作成できます。それぞれの定義には、OSPF 対応インタフェースに固有の複数のパラメータがあります。

OSPF インタフェース定義を作成するには、次の手順に従います。

1. **「*インタフェース*」タブで「*新規 OSPF インタフェース*」をクリックします。**
   「*新規 OSPF インタフェースの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このインターフェースを説明する名前を入力してください。

   インタフェース:この OSPF インタフェース定義と関連付けるインタフェースを選択します。

   認証タイプ:このインタフェースを介して送受信されるすべての OSPF パケットに対して使用する認証タイプを選択します。次の認証タイプを使用できます。

   - **MD5:**選択すると、MD5 認証が有効になります。MD5 (Message-Digest algorithm 5) とは、128ビットのハッシュ値を使用する一般的な暗号ハッシュ関数です。
   - **平文:**選択すると、平文認証が有効になります。パスワードはネットワーク上を平文の形で伝送されます。
   - **OFF:**選択すると、認証が無効になります。

   メッセージダイジェスト:この OSPF インタフェースに対して MD5 認証が使用されることを示すメッセージダイジェスト (MD) を選択します。ここでメッセージダイジェストを選択するためには、事前に「*メッセージダイジェスト*」タブでそのメッセージダイジェストを作成しておく必要があります。

   コスト:このインタフェースでデータパケットを送信するコスト。有効な値は 1～65535 の範囲内です。

詳細オプション(任意):「*詳細オプション*」チェックボックスを選択すると、追加の設定オプションが表示されます。

- **ハロー間隔:**Sophos UTM がこのインタフェースを介して Hello パケットを送信する頻度(秒)を指定します。デフォルト値は 10秒です。
- **再送間隔:**LSA(リンクステートアドバタイズメント)を受け取ったという確認応答がインタフェースに届かなかったときに、インタフェースが LSA を再送する頻度(秒)を指定します。デフォルト値は 5秒です。
- **デッド間隔:**Sophos UTM がこのインタフェースを介して Hello パケットの受信を待機する頻度(秒)を指定します。デフォルト値は 40秒です。原則的に、*Dead 間隔*の値は *Hello 間隔*の値の 4倍の長さにします。
- **プライオリティ:**ルータの優先順位を 1～255 の範囲の 8ビット値で指定します。この値は、特定のネットワークの指名ルータ(DR)を決定するために主に使用されます。デフォルト値は 1 です。
- **トランスミットディレイ:**インタフェースで LSU(リンク ステート アップデート)パケット送信に予想される頻度(秒)を指定します。範囲は1～65535 秒で、デフォルト値は 1 です。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   OSPF インタフェース定義が「*インタフェース*」タブに表示されます。

OSPF インタフェースを編集または削除するには、対応するボタンをクリックします。

ライブログを開く:OSPF ライブログには、OSPF インタフェースでのすべてのアクティビティが記録されます。ボタンをクリックして、新しいウィンドウでライブログを開きます。

6.7.4 メッセージダイジェスト

「*インタフェース & ルーティング > ダイナミックルーティング (OSPF) > メッセージダイジェスト*」タブでは、いわゆるメッセージダイジェストキーを生成することができます。メッセージダイジェストキーは、OSPF で MD5 認証を有効にするために必要です。MD5 認証では、パスワードを使用してメッセージダイジェストを生成します。これはデータパケットとパスワードの 128ビットのチェックサムです。メッセージダイジェストは、パスワードと関連付けられたキー ID とともにデータパケットで送信されます。

注 – 受信側ルータは、同じメッセージダイジェストキーで設定されていなければなりません。

メッセージダイジェストキーを作成するには、次の手順に従います。

1. **「*メッセージダイジェスト*」タブで「*新規メッセージダイジェストキー*」をクリックします。**
   「*メッセージダイジェストキーの新規作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   ID:このメッセージダイジェストキーのキー ID を入力します。範囲は 1～255 です。

   MD5 キー:関連するパスワードを入力します。最大 16文字の英数字から成る文字列にする必要があります。
3. **「*保存*」をクリックします。**
   新しいキーが「*メッセージダイジェスト*」リストに表示されます。

ダイジェストキーを編集または削除するには、対応するボタンをクリックします。

6.7.5 デバッグ

「*インタフェース＆ルーティング＞ダイナミックルーティング(OSPF)＞デバッグ*」タブでは、関連 OSPF パラメータについての詳細情報が別のブラウザウィンドウで表示されます。次の情報が含まれています。

- **OSPF ネイバーの表示:**OSPF ネイバー情報をインタフェースごとに表示するために使用します。
- **OSPF ルートの表示:**ルーティングテーブルの現在の状態を表示するために使用します。
- **OSPF インタフェースの表示:**OSPF 関連のインタフェース情報を表示するために使用します。
- **OSPF データベースの表示:**特定ルータの OSPF データベースに関連する情報を一覧表示するために使用します。
- **OSPF 境界ルータの表示:**ABR *(エリア境界ルータ)*と ASBR*(自律システム境界ルータ)*への内部 OSPF ルーティングテーブルのエントリを表示するために使用します。

6.7.6 詳細

「*インタフェース&ルーティング＞ダイナミックルーティング(OSPF)*」タブには、OSPF に関連する追加の設定オプションがあります。これらは、OSPF 以外のドメインから OSPF ドメインへのルーティング情報の再配布に関連するものです。

注 – ポリシールートを再分配することはできません。

直接接続されたネットワークを再配布:直接接続されているネットワークのルートを再配布する場合は、これを選択します。デフォルトのメトリック(コスト)値は 10です。

スタティックルートを再配布:スタティックルートおよびIPsec ルートを再分配する場合は、これを選択します。デフォルトのメトリック(コスト)値は 10です。

注 – IPsecトンネルを再配分するためにはストリクトルーティングを無効化する必要があります(「接続」の章を参照)。

BGP の再配布:BPG ルートを再分配する場合は、これを選択します。デフォルトのメトリック(コスト)値は 10です。

デフォルトルートを配布:デフォルトルートを OSPFドメインに再配布する場合は、これを選択します。

注 – デフォルトルートは、`0.0.0.0/0` へのルートの有無を問わず OSPFドメインにアドバタイズされます。

インタフェースリンク検知:インタフェースリンクが検出された場合のみにインタフェースのルートをアナウンスする場合は、これを選択します。

6.8 BGP

Border Gateway Protocol(BGP)とは、主にインターネットサービスプロバイダ(ISP)により、複数の自律システム(AS)間(つまりISP 間)の通信を可能にするために使用されるルーティングプロトコルで、インターネットのバックボーンになっています。自律システムは、1つ以上の ISP により制御され、内部ルーティングプロトコル(IGPなど)により接続された IP ネットワークの集合です。BGP はパスベクトル型プロトコルと形容されており、IGP と異なり、パス、ネットワークポリシ、ルールセットに基づいてルーティングを決定します。このために、ルーティングプロトコルではなく、可到達性プロトコルとみなすことができます。

各ISP(または他のネットワークプロバイダ)は、ネットワーク上でそれぞれの ISP を識別するために正式に登録された自律システム番号(ASN)を持つ必要があります。ISP は内部的に複数の自律システムをサポートすることができますが、インターネットにとってはルーティングプロトコルのみが重要になります。64512～65534 の範囲の番号の ASN はプライベートで、内部でのみ使用することができます。

BGP は伝送プロトコルとして TCP をポート 179 で使用します。

1つの AS のルータ間で BGP を使用する場合は、内部 BGP（iBGP）と呼ばれ、異なる AS のルータ間で BGP を使用する場合は外部 BGP（eBGP）と呼ばれます。

eBGP の利点は、ルーティングループを防止することで、IP パケットが AS を 2度通過することがありません。これは次の方法で実現します。特定のネットワークセグメントに到達するために IP パケットが通過する必要のあるすべての AS の全リストを、eBGP ルータが維持します。ルータは送信時に、近隣の eBGP ルータとこの情報を共有し、近隣の eBGP ルータも必要に応じてそれぞれのルーティングリストを更新します。eBGP ルータが既にこのような更新リストに存在することが検出された場合には、再度リストに追加されることはありません。

6.8.1 グローバル

「*Border Gateway Protocol > グローバル*」ページでは、UTMに対して BGP を有効または無効にすることができます。

1. **BGP を有効にするには、「ネイバー」ページで 1つ以上のネイバーを登録しておく必要があります。**
2. **「グローバル」ページで、BGP を有効にします。**
   トグルスイッチをクリックします。トグルスイッチがアンバー色になり、「*BGP システム*」セクションが編集可能になります。
3. **次の設定を行います。**
   AS 番号:システムの自律システム番号（ASN）を入力します。

   ルータ ID:ルータ ID として IPv4 アドレスを入力します。これはセッションの初期化中にネイバーに送信されます。

   ネットワーク:システムからネイバーにアナウンスするネットワークを追加または選択します。
4. **「*適用*」をクリックします。**

   トグルスイッチが緑色になり、BGP が有効になります。しばらくすると、「*概観*」セクションにステータス情報が表示されます。

6.8.2 システム

「*Border Gateway Protocol > システム*」ページでは、複数の自律システムの環境を作成できます。

注 – このページは、「*詳細*」ページで複数の AS の使用を有効にしている場合にのみアクセスできます。

新しい BGP システムを作成するには、次の手順に従います。

1. **「システム」ページで「*新規 BGP システム*」をクリックします。**
   「*BGP システムを新規作成*」ダイアログウィンドウが開きます。
2. **次の設定を行います。**
   名前:システムを説明する名前を入力してください。

   ASN:システムの自律システム番号(ASN)を入力します。

   ルータ ID:ルータ ID として IPv4 アドレスを入力します。これはセッションの初期化中にネイバーに送信されます。

   ネイバー:このシステムの AS に属するネイバーのチェックボックスにチェックを入れます。最初に「*ネイバー*」ページでネイバーを登録する必要があることに注意してください。

   ネットワーク:システムからアナウンスするネットワークを追加または選択します。

   インストールルート:このオプションはデフォルトで有効になっています。BGP ルータにルートを把握させる一方で、BGP ルーティングプロセスにはあまり関与させたくない場合のみに無効にしてください。複数の AS システムでこのオプションが選択されている場合、フィルタリストを作成して重複ネットワークが存在することがないようにしてください。そうしないと、同一ネットワークのルーティング動作が定義されなくなります。
3. **「*保存*」をクリックします。**
   システムが「システム」リストに表示されます。

6.8.3 ネイバー

「*Border Gateway Protocol* > *ネイバー*」ページでは、1つ以上の BGP ネイバールータを登録できます。ネイバールータ(ピアルータ)は、複数の自律システム(AS)間か 1つの AS 内で接続を構築します。2つのネイバー間での最初の通信時に、それぞれの BGP ルーティングテーブルが交換されます。その後は、ルーティングテーブルの変更に対する更新情報を相互に送信し、接続が確立していることを確認するためにキープアライブパケットを送信します。エラーが発生した場合には、通知パケットが送信されます。

BGP のポリシールーティングでは、受信ポリシーと送信ポリシーが異なります。このため、受信トラフィックと送信トラフィックに別々のルートマップとフィルタリストを定義して適用することができます。

「*グローバル*」ページで BGP を有効化できるようにするには、1つ以上のネイバールータを登録する必要があります。

新しい BGP ネイバーを登録するには、次の手順に従います。

1. **「ネイバー」ページで「*新規 BGP ネイバー*」をクリックします。**
「*BGP ネイバーを新規作成*」ダイアログウィンドウが開きます。

2. **次の設定を行います。**
名前:BGP ネイバールータの名前を入力します。

ホスト:ネイバーのホスト定義を追加または選択します。定義された IP アドレスが、UTMから到達できる必要があります。

リモート ASN:ネイバーの自律システム番号(ASN)を入力します。

認証:ネイバーで認証を必要とする場合、ドロップダウンリストから「*TCP MD5 シグニチャ*」を選択し、ネイバーに設定されているパスワードを入力します。

3. **必要に応じて次の詳細設定を行います。**
受信ルート/送信ルート:ルートマップを定義している場合、ここで選択できます。「*受信ルート*」または「*送信ルート*」を使用してルートマップを受信アナウンスメントまたは送信アナウンスメントに適用するかどうかを定義します。

受信フィルタ:/送信フィルタ:フィルタリストを定義している場合、ここで選択できます。「*受信フィルタ*」または「*送信フィルタ*」を使用してフィルタを受信アナウンスメントまたは送信アナウンスメントに適用するかどうかを定義します。

Next-Hop-Self:iBGP ネットワークでは、ルータが外部 eBGP ネットワークを内部的にアナウンスした場合、直接的な外部接続を持たない iBGP ルータはそのネットワークへのパケットのルーティング方法を把握していません。このオプションを選択すると、eBGP ルータは外部ネットワークに到達するための次のホップとして自らをアナウンスします。

マルチホップ: Cisco ルータは、2つの外部ピアを直接接続することを許可しないサードパーティ製ルータを使って、eBPG を実行できる場合があります。この接続を実現するには、eBGP マルチホップを使用します。eBGP マルチホップは、直接接続できない、2つの外部ピア間のネイバー接続を可能にします。マルチホップは、eBGP のみで機能し、iBGP では機能しません。

Soft-Reconfiguration:デフォルトで有効化されています。このオプションにより、ネイバーから送信される更新を保存することができます。

デフォルトルート生成:ネイバーにデフォルトルート 0.0.0.0 で送信します。ネイバーは、ルーティングテーブルに存在しないネットワークに到達するために必要な場合にのみ、このルートを使用します。

ウェイト: Cisco 専用のオプションです。このネイバーから学習したすべてのルートの汎用ウェイトを設定します。設定できる値は 0～65535 です。ウェイトが最も高いルートが、特定ネット

ワークに到達するために優先されます。ここで指定されたウェイトは、ルートマップのウェイトを上書きします。

4. **「*保存*」をクリックします。**
   ネイバーが「*ネイバー*」リストに表示されます。

6.8.4 ルートマップ

BGP では、ルートマップとは、ルートの再配布条件を設定し、ポリシールーティングを有効化するためのコマンドを指します。「*Border Gateway Protocol > ルートマップ*」ページでは、特定ネットワークのルートマップを作成し、メトリック、ウェイト、プリファレンス値を設定することができます。

どのルートを取るかを決定するベストパスアルゴリズムは次のように機能します。

1. ウェイトをチェックします。*
2. ローカルプリファレンスをチェックします。*
3. ローカルルートをチェックします。
4. AS パス長をチェックします。
5. 送信元をチェックします。
6. メトリックをチェックします。*

これはあくまでも簡素化した説明です。ベストパスの計算は非常に複雑であるため、詳しくはインターネット上の関連資料などを参照してください。

アスタリスク(*)が付いた項目は直接設定することができます。

BGP ルートマップを作成するには、次の手順に従います。

1. **「*ルートマップ*」ページで「*新規 BGP ルートマップ*」をクリックします。**
   「*BGP ルートマップを新規作成*」ダイアログウィンドウが開きます。

2. **次の設定を行います。**
   名前:ルートマップを説明する名前を入力します。

   マッチ基準:ルートマップの一致対象を特定ルータのIPアドレスにするか、AS 全体の IP アドレスにするかを選択します。

   - **IPアドレス;**「*ネットワーク*」ボックスに、フィルタを適用するホストまたはネットワークを追加または選択します。

- **AS 番号:**「*AS 正規表現*」ボックスに、フィルタを適用する AS 番号を定義するための BGP 正規表現を指定します。例:「`_100_`」を指定すると、AS100 を通過するすべてのルートが一致します。

ネットワーク:ルートマップを適応するネットワーク/ホストを追加または選択します。

メトリック:既定では、ルータがルートメトリックを動的に学習します。しかし、0～4294967295 の整数を使用して独自のメトリック値を設定できます。低いメトリック値の方が、高いメトリック値よりも優先されます。

加重:ベストパスの選択に使用されます。これは特定ルータに対して指定するもので、伝達されません。同じ宛先に複数のルートが存在する場合、高いウェイト値のルートが優先されます。ウェイトは最初に一致したASパスに基づき、0～4294967295 の整数で設定できます。

> **中** – ネイバーにウェイトが設定されている場合、指定されたネットワークへのルートが一致すると、このウェイトによってルートマップのウェイトが上書きされます。

プリファレンス:ローカル AS のすべてのルータのみに送信される AS パスのプリファレンス値を設定することができます。プリファレンス(ローカルプリファレンス)は、AS 外の特定ネットワークに到達するときに優先するパスを AS 内のルータに指示するものです。0～4294967295 の整数で設定でき、デフォルトは 100 です。

AS プリペンド:AS パスのプリペンドは、特定ルートを回避する上でプリファレンス設定が何らかの理由により充分でない場合に使用されます(メインルートが使用できない場合のみに取るべきバックアップルートなど)。これにより、自らの AS 番号を繰り返すことで(`65002 65002 65002`など)、AS パス属性を拡張することができます。BGP ルート選択では、最も短い AS パスが優先されるため、この選択に影響が及びます。AS プリペンドが設定されたルートマップを意図したとおりに機能させるには、ネイバーの「*送信ルート*」フィールドでルートマップを選択する必要があることに注意してください。

3. **「*保存*」をクリックします。**
   ルートマップが「*ルートマップ*」リストに表示されます。

これで、ネイバー定義にルートマップを使用することができます。

6.8.5 フィルタリスト

「*Border Gateway Protocol > フィルタリスト*」ページでは、IP アドレスまたは AS 番号に基づいてネットワーク間のトラフィックを制御するために使用するフィルタリストを作成できます。

フィルタリストを作成するには、次の手順に従います。

1. **「*フィルタリスト*」ページで「*新規 BGP フィルタリスト*」をクリックします。**
「*BGP フィルタリストを新規作成*」ダイアログウィンドウが開きます。

2. **次の設定を行います。**
名前:フィルタリストを説明する名前を入力します。

   フィルタ条件:フィルタの一致対象を特定ルータの IP アドレスにするか、AS 全体の IP アドレスにするかを選択します。

   - **IPアドレス:**「*ネットワーク*」ボックスに、フィルタを適用するホストまたはネットワークを追加または選択します。
   - **AS 番号:**「*AS 正規表現*」ボックスに、フィルタを適用する AS 番号を定義するための BGP 正規表現を指定します。例:「`_100_`」を指定すると、AS100 を通過するすべてのルートが一致します。

   ネットワーク:特定のネットワークに関する情報を拒否または許可するネットワーク/ホストを追加または選択します。

   アクション:ドロップダウンリストから、フィルタが一致した場合に取るアクションを選択します。トラフィックを拒否するか許可することができます。

   - **拒否:**「*ネイバー*」ページの「*受信フィルタ*」フィールドで特定ネイバーのネットワークを拒否した場合、UTM ではそのネットワークのアナウンスメントを無視します。「*送信フィルタ*」フィールドで特定ネイバーのネットワークを拒否した場合、UTMではそのネットワークのそのネイバーにアナウンスメントを送信しません。
   - **許可:**「*ネイバー*」ページの「*受信フィルタ*」フィールドで特定ネイバーのネットワークを許可した場合、UTM ではそのネットワークのアナウンスメントのみを受信します。「*送信フィルタ*」フィールドで特定ネイバーのネットワークを許可した場合、UTMではそのネットワークのそのネイバーのみにアナウンスメントを送信し、「*グローバル*」または「*システム*」ページで定義した他のネットワークには送信しません。

3. **「*保存*」をクリックします。**
フィルタリストが「*フィルタリスト*」リストに表示されます。

これで、ネイバー定義にフィルタリストを使用することができます。

6.8.6 詳細

「*BGP > 詳細*」ページでは、BGP の追加設定を行ったり、BGP デバッグ情報ウィンドウにアクセスすることができます。

複数の自律システムの許可

複数 ASを許可:複数 ASを設定するには、このチェックボックスにチェックを入れます。これによって、「*システム*」ページが有効になるため、複数の ASを追加することができます。同時に、「*グローバル*」ページの「*BGP システム*」セクションは無効になり、「*グローバル*」ページには、すべての AS に関する情報が表示されます。

厳密 IP アドレスマッチ

厳密 IP アドレスマッチ:IP アドレスの完全な一致を行うには、このチェックボックスにチェックを入れます。例:10.0.0.0/8 は 10.0.0.0/8 と一致しますが、10.0.1.0/24 には一致しません。

マルチパスルーティング

通常、コストが等しい複数のルートが存在する場合でも、使用できるルートパスは 1つのみです。これを選択すると、8つまでの等価ルートを同時に使用できるようになります。これにより複数のインタフェース間でのロードバランシングが可能になります。

BGP デバッグ

このセクションには、3つのデバッグ情報ウィンドウがあります。ボタンをクリックしてウィンドウを開きます。各ボタンの名前は、通常コマンドラインで呼び出す BGP コマンドに対応しています。ボタンをクリックすると、ウィンドウにそのコマンドの結果がコマンドライン出力形式で表示されます。

IP BGP ネイバーの表示:UTM のネイバー情報を表示します。各ネイバーのリンク状態が「*確立*」となっていることを確認します。

IP BGP ユニキャストの表示:優先パスを示す現在の BGP ルーティングテーブルが表示されます。これは、メトリック、ウェイト、プリファレンスの設定とその影響の概要を確認する上で特に有益です。

IP BGP サマリの表示:すべての BGP 接続のステータスが表示されます。この情報は、「*グローバル*」ページの「*BGP サマリ*」セクションにも表示されます。

6.9 マルチキャストルーティング (PIM-SM)

「*インタフェース & ルーティング > マルチキャストルーティング (PIM-SM)*」メニューを使用すると、ネットワーク上で使用する PIM-SM *(Protocol Independent Multicast Sparse Mode)*を設定することができます。PIM とは、複数ネットワーク内でマルチキャストパケットを動的 (ダイナミック) にルーティングするためのプロトコルです。マルチキャストとは、複数のクライアントが受信するパケットをできるだけ小さいトラフィックを使用して効率的に配信するための技術です。通常、複数のクライアント宛て

のパケットは、コピーされて各クライアントに個別に送信されるため、消費される帯域幅はユーザ数に応じて増大します。そのため、同じパケットを同時に要求する多数のクライアントを抱えるサーバ (コンテンツのストリーミング用サーバなど) の場合、大量の帯域幅が必要となります。

これに対しマルチキャストは、ネットワークの各リンク経由でパケットを一度だけ送信することにより帯域幅を節約します。これを実現するために、マルチキャストでは、サーバ (送信者) からクライアント (受信者) への経路上でいつコピーを作成するかを決定するために、適切に設定されたルータを使用します。これらのルータは、PIM-SM を使用してアクティブなマルチキャスト受信者を追跡し、ルーティングの設定にこの情報を使用します。

PIM-SM 通信の簡単な説明は次のとおりです。送信者がマルチキャストデータの送信を開始します。送信者用のマルチキャストルータが PIM-SM 経由で RP ルータに登録し、RP ルータは送信者のルータに Join メッセージを送信します。マルチキャストパケットが送信者から RP ルータに流れるようになります。受信者が、このマルチキャストグループの IGMP ブロードキャスト経由でローカル PIM-SM ルータに自己登録します。このルータは受信先用の Join 要求を RP ルータに向けて送信し、RP ルータはマルチキャストトラフィックを受信者に転送します。

マルチキャストは、独自の IP アドレス範囲 (224.0.0.0/4)を持ちます。

6.9.1 グローバル

「*マルチキャストルーティング (PIM-SM) > グローバル*」タブでは、PIM を有効または無効にできます。「*ルーティングデーモンの設定*」エリアには、関与するインタフェースとルータのステータスが表示されます。

PIM を有効にする前に、「*インタフェース*」タブで PIM インタフェースとして機能するインタフェースを 2つ以上定義して、「*RP ルータ*」タブでルータを 1台定義する必要があります。

PIM-SM を有効にするには、次の手順に従います。

1. **「*グローバル*」タブで PIM-SM を有効化します。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*ルーティングデーモン設定*」エリアが編集可能になります。

2. **次の設定を行います。**
   アクティブな PIM-SM インタフェース:PIM-SM に使用するインタフェースを 2つ以上選択します。インタフェースの設定は「*インタフェース*」タブで行います。

   アクティブな PIM-SM RP ルータ:PIM-SM に使用する RP ルータを 1つ以上選択します。RP ルータの定義は「*RP ルータ*」タブで行います。

3. **「*適用*」をクリックします。**
   設定が保存されます。ネットワークで PIM-SM 通信が有効になりました。

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。PIM-SM を無効にするには、緑色のトグルスイッチをクリックします。

ライブログ

「*ライブログを開く*」ボタンをクリックすると、新しいウィンドウで PIM ライブログが開きます。

6.9.2 インタフェース

「*マルチキャストルーティング (PIM-SM) > インタフェース (Interfaces)*」タブでは、どの Sophos UTM インタフェース上でマルチキャスト通信を行うかを定義することができます。

新しい PIM-SM インタフェースを作成するには、次の手順に従います。

1. **「*インタフェース*」タブで「*新規 PIM-SM インタフェース*」をクリックします。**
   「*新規 PIM-SM インタフェースの作成*」ダイアログウィンドウが開きます。

2. **次の設定を行います。**
   名前:PIM-SM インタフェースを説明する名前を入力します。

   インタフェース:PIM および IGMP ネットワークトラフィックを許可するインタフェースを選択します。

   DR 優先度 (任意):インタフェースの指定ルータ (DR) の優先順位を定義する番号を入力します。同じネットワークセグメント内に複数の PIM-SM ルータが存在する場合、優先順位が最も高いルータが IGMP 要求を受け付けます。0～2^{32} の数字を使用できます。優先順位を指定しないと、デフォルトで 0 が使用されます。

   IGMP:サポートする IGMP *(Internet Group Management Protocol)* のバージョンを選択します。IGMP は、受信者がマルチキャストグループのメンバシップを確立するために使用します。

   コメント (任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しい PIM-SM インタフェースがインタフェースリストに追加されます。

PIM-SM インタフェースを編集または削除するには、対応するボタンをクリックします。

6.9.3 RPルータ

ネットワーク上でマルチキャストを使用できるようにするためには、1つ以上のランデブーポイントルータ(RP ルータ)を設定する必要があります。RP ルータは、マルチキャスト受信者と送信者の両方から登録を受け付けます。RP ルータとは、特定のマルチキャストグループの RP ルータとして選ばれた通常の PIM-SM ルータでもあります。どのルータが RP ルータとなるかについて、すべての PIM-SM ルータが合意する必要があります。

RP ルータを作成するには、次の手順に従います。

1. **「*RP ルータ*」タブで「*新規ランデブーポイントルータ*」をクリックします。**
   「*新規 RP ルータの作成*」ダイアログウィンドウが開きます。

2. **次の設定を行います。**
   名前:RP ルータを説明する名前を入力します。

   ホスト:RP ルータとして機能するホストを作成(または選択)します。

   優先度:RP ルータの優先順位を定義する数字を入力します。優先順位が一番低い RP ルータに、Join メッセージが送信されます。0～255 の数字を使用できます。優先順位を指定しないと、デフォルトで 0 が使用されます。

   マルチキャストグループプレフィックス:RP ルータが担当するマルチキャストグループを入力します。RP ルータが複数のマルチキャストグループを担当する場合は、グループのプレフィックスを 224.1.1.0/24 のように定義できます。マルチキャストグループ(プレフィックス)は、マルチキャストアドレスの範囲内(224.0.0.0/4)にする必要があります。

   コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しい RP ルータがルータのリストに追加されます。

RP ルータを編集または削除するには、対応するボタンをクリックします。

6.9.4 ルート

受信者と送信者の間に、継続的な通信ルートをセットアップする必要があります。受信者、送信者、RP ルータが同じネットワークセグメント内にない場合、これらの間の通信を可能にするルートを作成する必要があります。

PIM-SM ルートを作成するには、次の手順に従います。

1. **「*ルート*」タブで、「*新規 PIM-SM ルート*」をクリックします。**
   「*新規 PIM-SM ルートの作成*」ダイアログウィンドウが開きます。

2. **次の設定を行います。**
   ルートタイプ:次のルートタイプを使用できます。

   - **インタフェースルート:**パケットは特定のインタフェース上で送信されます。これは 2つの状況で役立ちます。1つ目は、ゲートウェイの IP アドレスが不明になるダイナミック(動的)インタフェース(PPP)上でルーティングする場合です。2番目は、直接接続されたネットワークの外側にゲートウェイがあるデフォルトルートを定義する場合です。
   - **ゲートウェイルート:**パケットは特定のホスト(ゲートウェイ)へ送信されます。

   ネットワーク:PIM トラフィックをルーティングする宛先アドレス範囲を選択します。

   ゲートウェイ:ゲートウェイがデータパケットを転送するゲートウェイ/ルータを選択します(ルートタイプに「*ゲートウェイルート*」を選択した場合のみ使用可)。

   インタフェース:ゲートウェイがデータパケットを転送するインタフェースを選択します(ルートタイプに「*インタフェースルート*」を選択した場合のみ使用可能)。

   コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しい PIM-SM ルートがルートのリストに追加されます。

PIM-SM ルートを編集または削除するには、対応するボタンをクリックします。

6.9.5 詳細

「*インタフェース & ルーティング > マルチキャストルーティング (PIM-SM) > 詳細*」タブでは、PIM の詳細設定を構成することができます。

Shortest Path Tree(最短パスツリー)設定

一部のネットワークでは、送信者、RP、受信者の間のPIM通信ルートは可能な限り最短のネットワークパスとはなりません。「*SPTへの切り替えを有効にする*」オプションを使用すると、特定のトラフィックしきい値に達したときに送信者と受信者の間の既存の通信を最短パスに切り替えて、モデレータの RPを省くことができます。

自動ファイアウォール設定

このオプションを有効にすると、指定されたマルチキャストグループにマルチキャストトラフィックを転送するために必要となるすべてのファイアウォールルールがシステムによって自動的に作成されます。

デバッグ設定

PIM-SM ルーティングデーモンログに追加のデバッグ情報を表示するには、「*デバッグモードを有効化*」オプションを選択します。

7 ネットワークサービス

この章では、ご利用のネットワーク用にSophos UTMの複数のネットワークサービスを設定する方法を説明します。

この章では、次のトピックについて説明します。

- DNS
- DHCP
- NTP

7.1 DNS

「*ネットワークサービス > DNS*」メニューにあるタブには、さまざまな設定オプションがあり、すべて*ドメインネームシステム*(DNS)に関連しています。DNSとは、ドメイン名(コンピュータのホスト名)をIPアドレスに変換するために主に使用されるシステムです。

7.1.1 グローバル

「*ネットワークサービス > DNS > グローバル*」タブでは、UTMを再帰的なDNSリゾルバとして使用することを許可するネットワークを指定できます。ここでは通常、内部ネットワークを選択します。

注 – 内部DNSサーバをActive Directoryの一部などとしてすでに起動している場合、このボックスは空のまま残します。

DNSSEC

Domain Name System Security Extensions (DNSSEC)は、セキュリティを強化したDNSの拡張機能です。公開鍵暗号方式を使用してDNS参照レコードをデジタル署名することで機能します。この機能を選択しないと、UTMはすべてのDNSレコードを受け入れます。この機能を選択すると、UTMは、送信されるDNS要求のDNSSEC署名を検証します。正しく署名されたレコードのみが署名済みゾーンから許可されます。

注 – この機能を選択すると、DNSレコードは、手動でインストールされた、またはISPによって割り当てられたDNSSEC未対応のフォワーダに拒否される場合があります。この場合は、「フォ

ワーダ」タブで、ボックスから DNS フォワーダを削除し、「*ISP が割り当てたフォワーダを使用*」チェックボックスを無効にします。

リゾルバキャッシュをクリア

DNS プロキシでは、レコードに対してキャッシュを使用します。各レコードには有効期限（TTL、生存時間）があり、この時間にレコードは削除されます。通常は 1日に設定されています。ただし、キャッシュは手動で空にすることもできます（TTL が失効する前に DNS レコードの最新の変更を今すぐ有効にしたい場合など）。キャッシュを空にするには、「*今すぐリゾルバキャッシュをクリア*」をクリックします。

7.1.2 フォワーダ

「*ネットワークサービス > DNS > フォワーダ*」タブでは、いわゆる DNS フォワーダを指定できます。DNSフォワーダとは、ネットワーク上にある DNS *（ドメインネームシステム）*サーバであり、外部 DNS 名に関する DNS クエリを当該ネットワーク外の DNS サーバに転送（フォワーディング）するために使用します。可能な限り、設定に DNS フォワーダを追加してください。DNS フォワーダは、お客様のサイトの「近く」にあり、（可能であれば）同じインターネットプロバイダが提供しているホストにする必要があります。これは「親」キャッシュとして使用されます。これにより、DNS 要求の速度が飛躍的に向上します。転送を行うネームサーバを指定しないと、ゾーン情報についてのクエリ（問い合わせ）は最初にルート DNS サーバに対して行われるため、要求が完了するまで時間がかかります。

DNS フォワーダを選択するには、次の手順に従ってください。

1. **DNS フォワーダを選択します。**
   DNS フォワーダを選択または追加します。

   ISP が割り当てたフォワーダを使用（オプション）:DNS クエリを ISP の DNS サーバに転送する場合は、*ISP が割り当てたフォワーダを使用*チェックボックスにチェックを入れます。このチェックボックスにチェックを入れると、ISP によって自動的に割り当てられたすべてのフォワーダがボックスの下に一覧表示されます。

2. **「*適用*」をクリックします。**
   設定が保存されます。

7.1.3 リクエストルーティング

内部 DNS サーバが稼働しており、DNS フォワーダに解決させたくないドメインがある場合、そのドメインへのクエリをフォワーダではなく内部サーバに処理させることができます。「*ネットワークサービス > DNS > リクエストルーティング*」タブで、独自の DNS サーバへのルートを定義することができます。

DNS リクエストルートを作成するには、次の手順に従います。

1. **「*リクエストルーティング*」タブで「*新規 DNS リクエストルート*」をクリックします。**
   「*新規 DNS リクエストルートの作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   ドメイン:代替 DNS サーバを使用したいドメインを入力します。

   ターゲットサーバ:上記ステップで入力したドメインを解決するために使用する DNS サーバを 1つ以上選択します。

   コメント(任意):説明などの情報を追加します。
3. **「保存」をクリックします。**
   新しいルートが「*DNS リクエストルート*」リストに表示され、ただちに有効になります。

DNS リクエストルートを編集または削除するには、対応するボタンをクリックします。

7.1.4 スタティックエントリ

独自の DNS サーバをセットアップせず、ネットワーク内のいくつかのホストに対してスタティック DNS マッピングが必要な場合は、ここでこれらのマッピングを入力することができます。

UTM バージョン 9.1 から、この機能は「*定義とユーザ > ネットワーク定義*」タブに移動しました。DNS マッピングは該当するホストとともに定義されるようになりました。

「*スタティックエントリ*」ボタンをクリックすると、「*定義とユーザ*」>「*ネットワーク定義*」タブが開きます。自動的に、静的エントリのあるホストのみが表示されます。リストの上部のドロップダウンリストを使用すると、フィルタ設定を変更できます。

7.1.5 DynDNS

ダイナミック DNS(略して DynDNS)は、可変 IP アドレスを持つコンピュータに静的インターネットドメイン名を割り当てることを可能にするドメインネームサービスです。それぞれの DynDNS サービスプロバイダの Web サイトで DynDNS サービスにサインアップし、DNS エイリアスを取得すると、アップ

リンク IP アドレスの変化に応じてこのエイリアスが自動的に更新されます。このサービスに登録すると、設定に必要なホスト名、ユーザ名、パスワードが提供されます。

DynDNS を設定するには、次の手順に従ってください。

1. **「*DynDNS*」タブで、「*新規 DynDNS*」をクリックします。**
   「*新規 DynDNS の作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   タイプ:次の DynDNS サービスを使用できます。

   - **DNS Park:**公式ウェブサイト:www.dnspark.com
   - **DtDNS:**公式ウェブサイト:www.dtdns.com
   - **DynDNS:**サービスプロバイダ、Dynamic Network Services Inc (Dyn) の標準 DNS サービス。公式ウェブサイト:www.dyndns.com
   - **DynDNS-custom:**サービスプロバイダ、Dynamic Network Services Inc (Dyn) のカスタム DNS サービス (www.dyndns.com)。カスタムDNSは、主にユーザ自身が所有または登録しているドメインを使用するために設計されています。
   - **easyDNS:**公式ウェブサイト:www.easydns.com
   - **FreeDNS:**公式ウェブサイト:freedns.afraid.org
   - **Namecheap:**公式ウェブサイト:www.namecheap.com
   - **zoneedit:**公式ウェブサイト:www.zoneedit.com

   注 –「*サーバ*」フィールドには、UTMが IP の変更を送信する URL が表示されます。

   割り当て (「*FreeDNS*」タイプには無効):DynDNS 名を関連付ける IP アドレスを定義します。ローカルインタフェースがパブリック IP アドレスを持つ場合は、この*ローカルインタフェースの IP* を選択すると便利です。通常は、DSL アップリンクに対してこのオプションを使用します。「*デフォルトルートの最初のパブリック IP*」を選択する場合、インタフェースの指定は不要です。代わりに、UTMがパブリック DynDNS サーバに WWW 要求を送信し、パブリック DynDNS サーバは現在使用中のパブリックIPを返します。これは、プライベートネットワーク内部にあるUTMがパブリック IP アドレスを持っておらず、マスカレーディングルータ経由でインターネットに接続している場合に有用です。

   注 – FreeDNS は、常にデフォルトルートの最初のパブリック IP アドレスを使用します。

インタフェース(「*FreeDNS*」タイプでは無効、「*ローカルインタフェースの IP*」のみ):DynDNS サービスを使用するインタフェースを選択します。最も可能性が高いのは、インターネットに接続された外部インタフェースです。

ホスト名:DynDNS サービスプロバイダから受け取ったドメイン名を入力します(`example.dyndns.org` など)。ここでは、特定の構文を遵守してホスト名を入力する必要はありません。ここで入力が必要な内容は、各 DynDNS サービスプロバイダの要件に応じて異なります。DynDNS ホスト名をゲートウェイのメインホスト名として使用することもできますが、必須ではありません。

エイリアス(オプション):このダイアログボックスは、前述のメインホスト名と同じ IP アドレスをポイントする追加ホスト名を入力するために使用します(`mail.example.com`、`example.com` など)。

MX(オプション、「*DNS Park*」、「*DynDNS*」、「*easyDNS*」タイプのみ):MX(mail exchanger)は、ホスト名で指定されたサーバ以外の特定サーバにメールを送信するために使用します。MX レコードは、特定ドメインへのメールの送信先となるホスト(サーバ)を指定するという目的のために使用します。たとえば、MX として `mail.example.com` を指定すると、`user@example.com` 宛てのメールはホストである `mail.example.com` に配信されます。

MX 優先順位(オプション、「*DNS Park*」タイプのみ):ドメインへのメールの配信に指定したメールサーバを優先するかどうかを示す正の整数値を入力します。数値が低いサーバが数値の高いサーバよりも優先されます。DNS Park では、デフォルト値として 5 が使用され、これがほとんどの目的に適っているため、このフィールドを空白のままにすることができます。MX の優先順位の詳細な技術情報については、RFC 5321 を参照してください。

バックアップ MX(オプション、「*DynDNS*」または「*easyDNS*」タイプのみ):「*ホスト名*」テキストボックスで指定したホスト名がメイン MX となる場合のみ、このチェックボックスにチェックを入れます。すると、「*MX*」テキストボックスのホスト名はバックアップ MX としてのみアドバタイズされます。

ワイルドカード(オプション、「*DynDNS*」または「*easyDNS*」タイプのみ):このオプションは、登録したドメインと同じ IP アドレスをサブドメインのポイント先とする場合に選択します。このオプションを使用すると、ドメインにワイルドカードとしてアスタリスク(*)が追加されます(`*.example.dyndns.org` など)。これにより、`www.example.dyndns.org` などが `example.dyndns.org` と同じアドレスをポイントするようになります。

ユーザ名:DynDNS サービスプロバイダから受け取ったユーザ名を入力します。

パスワード:DynDNS サービスプロバイダから受け取ったパスワードを入力します。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しい DynDNS が「*DynDNS*」リストに表示されます。サービスは無効になっています(トグルスイッチは灰色)。

4. **DynDNS を有効にします。**
   DynDNS サービスを有効にするには、トグルスイッチをクリックします。

   これでサービスが有効になります(トグルスイッチは緑色)。

DynDNS を編集または削除するには、対応するボタンをクリックします。

複数の DynDNS オブジェクトを同時に使用することができます。2つのホスト名のすべての設定が同じであれば、別オブジェクトを 2つ作成するのではなく、「*エイリアス*」オプションを使用することを推奨します。

7.2 DHCP

DHCP (*Dynamic Host Configuration Protocol*) は、定義された IP アドレスプールからクライアントコンピュータにアドレスを自動的に割り当てます。大規模ネットワークにおけるネットワーク設定を簡素化し、アドレスの衝突を防止するために設計されています。DHCP はクライアントに、IP アドレス、デフォルトのゲートウェイ情報、DNS 設定情報を割り当てます。

クライアントコンピュータの設定を簡素化し、モバイルコンピュータが複数のネットワークを問題なく行き来できるようにすることに加え、DHCP は IP アドレスに関連する問題の原因特定とトラブルシューティングもサポートします。これは、DHCP サーバ自体の設定に問題があることが多いためです。また、アドレスを必要に応じて割り当てて、不要な場合は再利用することができるため、すべてのコンピュータが同時にアクティブになっていない場合などに、アドレススペースの使用をより効率化することができます。

7.2.1 サーバ

「*ネットワークサービス > DHCP > サーバ*」タブを使用すると、DHCP サーバを設定することができます。Sophos UTMは、接続されたネットワークだけでなく、他のネットワークに対して DHCP サービスを提供します。DHPC サーバを使用して、クライアントに基本ネットワークパラメータを割り当てることができます。独自の構成を持つそれぞれ独自のインタフェースとネットワークを取得して、複数のインタフェース上で DHCP サービスを実行できます。

注 –「*オプション*」タブでは、クライアントに送信する追加 DHCP オプションまたは異なる DHCP オプションを定義できます。「*オプション*」タブに定義された DHCP オプションは、そのスコープがグローバルに設定されていない場合、「サーバ」タブの設定を上書きします。たとえば、選択したホストのみに DHCP オプションを定義するときに、DHCP サーバに定義されたものとは異なる DNS サーバまたはリース期間を割り当てることができます。

DHCP サーバを設定するには、次の手順に従ってください。

1. **「サーバ」タブで、「*新規 DHCP サーバ*」をクリックします。**
   「*新規 DHCP サーバを作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   インタフェース:IP アドレスをクライアントに割り当てるインタフェース。すでに設定されているインタフェースのみを選択できます。

   アドレスタイプ:このオプションは IPv6 をグローバルに有効にしている場合にのみ使用できます。DHCP サーバの IP バージョンを選択します。

   レンジの先頭/末尾:そのインタフェースのアドレスプールとして使用する IP レンジ。デフォルトで、ネットワークカードに設定されたアドレスエリアがテキストボックスに表示されます。クライアントが同じネットワーク内にある場合、レンジはインタフェースが接続されたネットワーク内にする必要があります。クライアントが別のネットワークにある場合、レンジはリレーされたDHCP要求の送信元ネットワーク内にする必要があります。

   注 – 定義した DHCP IP 範囲が大きければ大きいほど、UTM によって、より多くのメモリが予約されます。DHCP 範囲を適切な値に削減するようにしてください。許可される最大範囲は、/9 ネットワークです。

   DNS サーバ 1/2:DNS サーバの IP アドレス。

   デフォルトゲートウェイ (IPv4 のみ):デフォルトゲートウェイ の IP アドレス。

   注 – ワイヤレスアクセスポイントと RED アプライアンスの両方で、デフォルトゲートウェイが接続先インタフェースと同じサブネット内にある必要があります。

   ドメイン (任意):クライアントに送信されるドメイン名を入力します (例: `intranet.example.com`)。

リース期間 (IPv4 のみ):DHCP クライアントがリースの更新を自動的に試行します。このリース期間中にリースが更新されない場合、IP アドレスリースの期限が切れます。ここでは、その間隔を秒数で定義できます。デフォルトは 86,400秒 (1日) です。最小値は 600秒 (10分) で、最大値は 2,592,000秒 (1か月) です。

有効期間 (IPv6 のみ):DHCP クライアントがリースの更新を自動的に試行します。この有効期間中にリースが更新されない場合、IP アドレスリースステータスが無効になり、アドレスがインタフェースから削除され、他に割り当てられるようになります。間隔は 5分から無限の間で選択できますが、有効期間は推奨期間以上にする必要があります。

推奨期間 (IPv6 のみ):DHCP クライアントがリースの更新を自動的に試行します。この推奨期間中にリースが更新されない場合、IP アドレスリースステータスがデプリケート、つまり引き続き有効ではあるものの、新しい接続には使用されないようになります。間隔は、5分から無限の間で選択できます。

3. **次の詳細設定を任意で行います。**

WINS ノードタイプ (IPv4 のみ):*Windows Internet Naming Service* WINS とは、マイクロソフトが Windows に実装した *NetBIOS Name Server* (NBNS) であり、NetBIOS コンピュータ名用のネームサーバおよびサービスです。WINS サーバは、コンピュータ名を IP アドレスと一致させるデータベースとして機能するため、NetBIOS を使用しているコンピュータが TCP/IP ネットワークのメリットを利用できるようになります。次の WINS ノードタイプを使用できます。

- **設定しない:**WINS ノードタイプは設定するのではなくクライアントに選択されます。
- **Bノード (WINS なし):**Bノードシステムはブロードキャストのみを使用します。
- **Pノード (WINS のみ):**Pノードシステムは WINS (Windows name server) へのポイントツーポイントの名前問い合わせのみを使用します。
- **Mノード (ブロードキャスト後 WINS):**Mノードシステムは、まずブロードキャストしてから、ネームサーバに問い合わせを行ないます。
- **Hノード (WINS 後ブロードキャスト):**Hノードシステムは、まずネームサーバに問い合わせてから、ブロードキャストします。

WINS サーバ:選択した WINS ノードタイプに応じて、このテキストボックスが表示されます。WINS サーバの IP アドレスを入力します。

スタティックマッピングされたクライアントのみ (オプション):スタティック DHCP マッピングを持つクライアントのみに DHCP サーバが IP アドレスを割り当てるようにするには、このオプションを選択します (*「定義とユーザ」>「ネットワーク定義」>「ネットワーク定義」*参照)。

HTTP プロキシ自動設定の有効化:ブラウザの自動プロキシ設定用に PAC ファイルを提供するには、このオプションを選択します。詳しくは、「*Web プロテクション > Web フィルタリング > 詳細*」の章で、「*プロキシの自動設定*」セクションを参照してください。

注 – Microsoft Windows では現在、IPv6 で HTTP プロキシの自動設定をサポートしていません。

DHCP リレー経由のクライアント:これを選択すると、DHCP サーバは接続されたインタフェースのネットワーク内に存在しないクライアントに IP アドレスを割り当てます。この場合、上に定義されたアドレスレンジは、接続されたインタフェースのネットワーク内ではなく、リレーされた DHCP 要求の転送元ネットワーク内にする必要があります。

ネットマスク:リレーされた DHCP 要求の転送元ネットワークのネットマスクを選択します。

コメント(任意):説明などの情報を追加します。

4. **「保存」をクリックします。**
新しい DHCP サーバ定義が DHCP サーバのリストに表示され、ただちにアクティブになっています。

DHCP サーバ定義を編集または削除するには、対応するボタンをクリックします。

7.2.2 リレー

「*ネットワークサービス > DHCP > リレー*」タブでは、DHCP リレーを設定することができます。DHCP サービスは別の DHCP サーバによって提供され、UTMはリレーとして機能します。DHCP リレーを使用すると、ネットワークセグメントをまたいで DHCP 要求および応答を転送することができます。DHCP サーバと、DHCP トラフィックが転送されるインタフェースのリストを指定する必要があります。

DHCP リレーを設定するには、次の手順に従ってください。

1. **「*リレー*」タブで、「*DHCP リレー*」を有効にします。**
トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*DHCP リレーの設定*」エリアが編集可能になります。

2. **DHCP サーバを選択します。**

3. **該当するインタフェースを追加します。**
   インタフェースを DHCP サーバに追加するとともに、すべてのインタフェースを DHCP の要求と応答が転送されるクライアントのネットワークに追加します。

4. **「*適用*」をクリックします。**
   設定が保存されます。

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

7.2.3 スタティックマッピング

一部または全部のクライアントの IP アドレスとクライアント間の静的マッピングを作成できます。UTM バージョン 9.1 から、この機能は「*定義とユーザ > ネットワーク定義*」タブに移動しました。DHCP マッピングは該当するホストとともに定義されるようになりました。

「*スタティックマッピング*」ボタンをクリックすると、「*定義とユーザ > ネットワーク定義*」タブが開きます。自動的に、静的マッピングのあるホストのみが表示されます。リストの上部のドロップダウンリストを使用すると、フィルタ設定を変更できます。

7.2.4 IPv4 リーステーブル

DHCP を使用すると、クライアントは IPアドレスを持つのではなく、DHCP サーバから IP アドレスを*借りる(リースする)*ことになります。これにより、アドレスを一定期間にわたって使用する許可をクライアントに与えます。

「*ネットワークサービス > DHCP > IPv4 リーステーブル*」タブにあるリーステーブルには、DHCP サーバが現在発行しているリースが、開始日付やリースの有効期限日などの情報とともに表示されます。

スタティックマッピングを追加して新規のホストを定義

既存のリースをスタティック MAC/IP マッピングのテンプレートとして使用し、ホストの定義に使用できます。以下の手順に従ってください。

1. **望ましいリースの「*静的化*」列の「*静的化*」ボタンをクリックします。**
   「*静的化*」ダイアログウインドウが開きます。

2. **次の設定を行います。**
   アクション:「*新規ホストの作成*」を選択します。

   名前:新規ホストを説明する名前を入力します。

DHCP サーバ:静的マッピングに使用するDHCP サーバを選択します。該当するDHCP の範囲がドロップダウンリストの下に表示されます。

IPv4 アドレス:DHCP プール範囲外のアドレスにIP アドレスを変更します。

注 – リースをスタティックマッピングに変換する場合、DHCP プールの範囲外の IP アドレスに変更する必要があります。ただし、IP アドレスを変更しても、クライアントの使用するアドレスはすぐには変更されず、次にリース更新を行うまで変更されません。

DNS ホスト名:DNS ホスト名を指定すると、ホストの静的 DNS エントリとして使用されます。

リバース DNS:ホストの IP アドレスと名前のマッピングを有効化するには、チェックボックスにチェックを入れます。同じIP アドレスに複数の名前をマッピングすることが可能ですが、1つの名前に対しては 1つの IPアドレスしかマッピングできません。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   設定が保存されます。

静的マッピングによる新しいホストは「*定義とユーザ > ネットワーク定義*」タブに表示されます。

スタティックマッピングを既存のホストに追加する

既存のリースを新しいスタティック MAC/IP マッピングのテンプレートとして使用し、ホストの定義に使用できます。以下の手順に従ってください。

1. **望ましいリースの「*静的化*」列の「*静的化*」ボタンをクリックします。**
   「*静的化*」ダイアログウインドウが開きます。

2. **次の設定を行います。**
   アクション:「*既存のホストを使用*」を選択します。

   ホスト:「フォルダ」アイコンをクリックして、ホストを追加します。

3. **「*保存*」をクリックします。**
   設定が保存されます。

静的マッピングによるホストは、「*定義とユーザ > ネットワーク定義*」タブに表示されます。

7.2.5 IPv6 リーステーブル

DHCP を使用すると、クライアントは IP アドレスを持つのではなく、DHCP サーバから IP アドレスを*借りる(リースする)*ことになります。これにより、アドレスを一定期間にわたって使用する許可をク

ライアントに与えます。

「*ネットワークサービス > DHCP > IPv6 リーステーブル*」タブにあるリーステーブルには、DHCP サーバが現在発行しているリースが、開始日付やリースの有効期限日などの情報とともに表示されます。

注 – プレフィックス広告経由で付与されたリースはテーブルに表示されません。

スタティックマッピングを追加して新規のホストを定義

既存のリースをスタティック MAC/IP マッピングのテンプレートとして使用し、ホストの定義に使用できます。以下の手順に従ってください。

1. **望ましいリースの「*静的化*」ボタンをクリックします。**
   「*静的化*」ダイアログウインドウが開きます。
2. **次の設定を行います。**
   アクション:「*新規ホストの作成*」を選択します。

   名前:新規ホストを説明する名前を入力します。

   DHCP サーバ:静的マッピングに使用する DHCP サーバを選択します。該当する DHCP の範囲がドロップダウンリストの下に表示されます。

   IPv6 アドレス:DHCP プール範囲外のアドレスに IP アドレスを変更します。

   注 – リースをスタティックマッピングに変換する場合、DHCP プールの範囲外の IP アドレスに変更する必要があります。ただし、IP アドレスを変更しても、クライアントの使用するアドレスはすぐには変更されず、次にリース更新を行うまで変更されません。

   DNS ホスト名:DNS ホスト名を指定すると、ホストの静的 DNS エントリとして使用されます。

   リバース DNS:ホストの IP アドレスと名前のマッピングを有効化するには、チェックボックスにチェックを入れます。同じ IP アドレスに複数の名前をマッピングすることが可能ですが、1 つの IP アドレスには1つの名前にしかマッピングできません。

   コメント(任意):説明などの情報を追加します。
3. **「*保存*」をクリックします。**
   設定が保存されます。

スタティックマッピングを既存のホストに追加する

既存のリースを新しいスタティック MAC/IP マッピングのテンプレートとして使用し、ホストの定義に使用できます。以下の手順に従ってください。

1. **望ましいリースの「*静的化*」列の「*静的化*」ボタンをクリックします。**
   「*静的化*」ダイアログウインドウが開きます。
2. **次の設定を行います。**
   アクション:「*既存のホストを使用*」を選択します。

   ホスト:「フォルダ」アイコンをクリックして、ホストを追加します。
3. **「保存」をクリックします。**
   設定が保存されます。

静的マッピングによるホストは、「*定義とユーザ > ネットワーク定義*」タブに表示されます。

7.2.6 オプション

「*ネットワークサービス > DHCP > オプション*」タブを使用すると、DHCP オプションを設定することができます。DHCP オプションは、DHCP サーバによりDHCP クライアントに提供される追加設定パラメータです。

例:一部の VoIP 電話の場合、DHCP サーバから必要な情報を提供するために、このページで 3つの追加 DHCP オプションを作成して有効にする必要があります。

- *ファイル名*:ブートファイルの名前。
- *次のサーバ*:ブートファイルを提供する TFTP サーバの名前。
- *4 (タイムサーバ)*:タイムサーバの IP アドレス。

DHCPオプションに異なるスコープを許可:選択したホストのみに提供するか、選択したサーバからのみとするか、グローバルにすることもできます。このため、同じホストに異なるパラメータを定義することができます。一部の DHCP オプションは、DNS サーバ (オプション6) など、「*DHCP > サーバ*」タブに既に定義されています。パラメータ値が一致しない場合、次の優先順位でパラメータがクライアントに提供されます。

1. スコープが「*ホスト*」の DHCP オプション
2. スコープが「*MAC プレフィックス*」の DHCP オプション
3. スコープが「*ベンダ ID*」の DHCP オプション
4. スコープが「*サーバ*」の DHCP オプション

5. DHCP サーバパラメータ(*DHCP > サーバ*」タブ)
6. スコープが「*グローバル*」の DHCP オプション

注 – DHCP 要求では、DHCP クライアントが処理できる DHCP オプションに関する情報を送信します。その結果、DHCP サーバは、ここに定義されたオプションに関係なく、クライアントが理解できる DHCP オプションのみを提供します。

DHCP オプションを作成するには、次の手順に従います。

1. **「*新規 DHCP オプション*」をクリックします。**
「*新規 DHCP オプションの作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
アドレスタイプ(IPv6 が有効な場合のみ):DHCP オプションを作成する IP バージョンを選択します。

   コード:作成する DHCP オプションのコードを選択します。

   注 –「*ファイル名*」エントリでは、そこで実行する DHCP クライアントにロードするファイルを指定できます。「*次のサーバ*」では、ブートサーバを定義できます。番号の DHCP オプションコードは、RFC 2132 などで定義されています。

   名前:このオプションを説明する名前を入力します。

   タイプ:コメントが「*(不明)*」のコードを選択した場合にのみ使用できます。オプションのデータタイプを選択します。データタイプには、「*IP アドレス*」、「*テキスト*」、「*16 進*」を使用できます。選択したデータタイプに応じて、対応する下のフィールドに適切なデータを入力します。

   アドレス:この DHCP オプションで DHCP クライアントに送信するホストまたはネットワークグループの IP アドレスを選択します。

   テキスト:この DHCP オプションで DHCP クライアントに送信するテキストを入力します。「*ファイル名*」コードでは、ここにファイル名を入力できます。

   16進:この DHCP オプションで DHCP クライアントに送信する 16 進値を入力します。16 進数をコロンで 2桁の区切ってまとめた形式で指定します(`00:04:76:16:EA:62` など)。

   スコープ:DHCP オプションを送信する条件を定義します。

- **グローバル:**DHCP オプションが定義されているすべての DHCP サーバによりすべての DHCP クライアントに送信されます。
- **サーバ:**「*サーバ*」ボックスには、DHCP オプションを送信する DHCP サーバを選択します。ボックスには、「*DHCP サーバ*」タブに定義されているすべての DHCP サーバが表示されます。
- **ホスト:**「*ホスト*」ボックスには、DHCP オプションが提供されるホストを追加または選択します。
- **MAC プレフィックス:**MAC プレフィックスを入力します。MAC アドレスが一致するすべての DHCP クライアントに DHCP オプションが提供されます。
- **ベンダー ID:**ベンダー ID またはベンダー ID のプレフィックスを入力します。この文字列に一致するすべての DHCP クライアントに DHCP オプションが提供されます。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
「*DHCP オプション*」リストに新しい DHCP オプションが表示され、直ちにアクティブになります。

DHCP オプションを編集または削除するには、対応するボタンをクリックします。

7.3 NTP

「*ネットワークサービス > NTP*」メニューを使用すると、接続されたネットワーク用の NTP サーバを設定することができます。*NTP*(Network Time Protocol)とは、IP ネットワーク経由でコンピュータシステムのクロックの同期をとるために使用するプロトコルです。Sophos UTMの時刻の同期(「*マネジメント > システム設定 > 日付と時刻*」タブで設定)だけではなく、特定のネットワークがこのサービスを使用できるように明示的に許可することもできます。

特定のネットワークに対して NTP による時刻同期を有効にするには、次の手順に従ってください。

1. **NTP サーバを有効にします。**
トグルスイッチをクリックします。
2. **「*許可ネットワーク*」を選択します。**
NTP サーバへのアクセスを許可するネットワークを選択します。
3. **「*適用*」をクリックします。**
設定が保存されます。

8 ネットワークプロテクション

この章では、Sophos UTMの基本的なネットワークプロテクション機能を設定する方法を説明します。WebAdmin の「*ネットワークプロテクション統計*」ページには、送信元ホストと宛先ホストの両方に対する侵入防御イベントおよび破棄されたデータパケットの概要が表示されます。各セクションには「*詳細*」リンクがあります。リンクをクリックするとWebAdmin の該当するレポートセクションが表示され、詳細な統計情報を参照できます。

この章では、次のトピックについて説明します。

- ファイアウォール
- ネットワークアドレス変換 (NAT)
- 侵入防御(IPS)
- サーバロードバランシング
- ボイスオーバー IP (VoIP)
- 詳細設定

8.1 ファイアウォール

「*ネットワークプロテクション > ファイアウォール*」メニューを使用すると、ゲートウェイのファイアウォールルールを定義し、管理することができます。一般的に、ファイアウォールはゲートウェイの中核部分で、ネットワーク環境においてセキュリティポリシーで禁止されている通信を妨げます。デフォルトの Sophos UTM の セキュリティポリシーでは、ゲートウェイの他のソフトウェアコンポーネントが機能するために必要な、自動的に生成されたルールセットを除くすべてのネットワークトラフィックをブロックしてログします。ただし、自動的に生成されたルールセットは「*ファイアウォール > ルール*」タブには表示されません。このポリシーでは、どのデータトラフィックにゲートウェイの通過を許可するかを明確に定義する必要があります。

8.1.1 ルール

「*ネットワークプロテクション > ファイアウォール > ルール*」タブでは、ファイアウォールルールセットを管理できます。デフォルトでは、タブを開くと、ユーザが作成したファイアウォールのルールのみが表示されます。リストの上部のドロップダウンリストを使用して、自動ファイアウォールルールのみ、または両方のタイプのルールを表示することを選択できます。自動ファイアウォールルール

は、区別しやすいように背景色とともに表示されます。自動ファイアウォールルールは、IPsec や SSL 接続を作成する場合など、いずれかの設定の「*自動ファイアウォールルール*」チェックボックスで選択した自動ファイアウォールルールに基づいて UTM によって生成されます。

新規に定義したすべてのファイアウォールルールは、ルールテーブルに追加されると、デフォルトで無効になります。自動ファイアウォールルール、および有効化されたユーザ作成のファイアウォールルールは、最初のルールが一致するまで、所定の順序で適用されます。自動ファイアウォールルールは、常にリストの最上部に表示されます。ユーザ作成のファイアウォールルールの処理順序は位置番号によって決まるため、位置番号によってルールの順序を変更すると、処理順序も変わります。

警告 – ファイアウォールルールが一致すると、他のすべてのルールは無視されます。そのため、ルールの順番は非常に重要です。「*すべて(送信元)*」–「*すべて(サービス)*」–「*すべて(宛先)*」–「*許可*」のようなルールは、ルールテーブルの上部には配置しないでください。このようなルールをルールテーブルの上部に配置すると、各パケットがゲートウェイを双方向に通過できるようになり、以降の他のルールはすべて無視されます。

ファイアウォールルールを作成するには、次の手順に従います。

1. **「*ルール*」タブで、「*新規ルール*」をクリックします。**
   「*新規ルール作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   グループ:「*グループ*」オプションは、複数のルールを論理的にグループ化するのに便利です。リストの上部のドロップダウンリストを使用して、グループごとにルールをフィルタリング表示できます。グループ化は表示用のみで、ルールの一致には関係ありません。新しいグループを作成するには、「*<< 新規グループ >>*」エントリを選択し、グループを説明する名前を「*名前*」に入力します。

   優先順位:優先順位番号。これによってルールの優先順位が定義されます。番号が小さいほど優先順位が高くなります。ルールは昇順に照合されます。あるルールが一致すると、それ以降、それより大きい番号のルールは評価されません。

   送信元:パケットの送信元のホストまたはネットワークを説明する送信元ネットワークの定義を追加します。

   サービス:プロトコルを説明するサービス定義を追加します。TCP または UDP の場合は、パケットの送信元および宛先ポートになります。

   宛先:パケットのターゲットホストまたはネットワークを説明する宛先ネットワークの定義を追加します。

注 – 1つ以上の送信元、サービスと、もしくは送信先を選択した場合、このルールは全ての適合可能な送信元–サービス–送信先の組み合わせに対して適用されます。例えばルールが 2つの送信元、2つのサービス、2つの送信先と適合した場合、8つのルールと同一となることもあります。これはそれぞれの送信元と送信先が両方のサービスを利用している場合です。

アクション:アクションは、ルールに一致したトラフィックに対する処理を説明します。次のアクションを選択できます。

- **許可:**接続を許可し、トラフィックを送ります。
- **破棄:**このアクションが指定されたルールと一致したパケットは、警告なしでドロップされます。
- **拒否:**このアクションが指定されたルールと一致した接続要求はアクティブに拒否されます。送信者には ICMP メッセージで通知されます。

コメント(任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   時間帯:デフォルトでは、時間帯は選択されていません。つまり、ルールは常に有効です。期間定義を選択すると、期間定義で指定された期間だけルールが有効になります。詳細は、*時間帯定義*を参照してください。

   トラフィックをログ:このオプションを選択すると、ログが有効になり、ルールに一致したパケットがファイアウォールログにログされます。

   送信元 MAC アドレス:パケットの送信元を説明する MAC アドレス定義を選択します。選択すると、ここで送信元 MAC アドレスが定義されている場合のみ、パケットはルールに一致します。MAC アドレスリストと送信元ネットワーク「*任意*」は、同時に指定できないことに注意してください。MAC アドレスリストの定義は、「*定義とユーザ > ネットワーク定義 > MAC アドレス定義*」タブで定義します。

4. **「*保存*」をクリックします。**
   新しいルールが「*ルール*」リストに表示されます。

5. **ファイアウォールルールを有効にします。**
   新しいルールはデフォルトで無効になっています(トグルスイッチはグレー表示)。ルールを有効にするには、トグルスイッチをクリックします。

   これでルールが有効になります(トグルスイッチは緑色)。

ルールを編集または削除するには、対応するボタンをクリックします。

ライブログを開く:フィルタされたパケットのリアルタイムログを含むポップアップウィンドウを開きます。表示は定期的に更新されて、最新のネットワークアクティビティが示されます。適用されたアクションによって、背景色が次のように変化します。

- 赤色:パケットは破棄されました。
- 黄色:パケットは拒否されました。
- 緑色:パケットは許可されました。
- グレー:アクションを決定できませんでした。

ライブログには、パケットが拒否される原因となったファイアウォールルールに関する情報も含まれます。こうした情報はルールのデバッグに不可欠です。
検索機能を使用して、特定エントリについてファイアウォールログをフィルタできます。検索機能では、表現の前にダッシュ(-)を付けることで、その表現を無効にできます。たとえば、`-WebAdmin`と指定すると、この表現を含むすべての行を連続して非表示にできます。

「*自動スクロール*」チェックボックスにチェックを入れると、ウィンドウのスクロールバーが自動的にスクロールダウンして、常に最新の結果が表示されます。

以下に、ファイアウォールの設定に関する基本的なヒントをいくつか示します。

- **破棄したブロードキャスト:**デフォルトでは、すべてのブロードキャストは破棄され、ログもされません(詳細は詳細を参照)。この機能は NetBIOS(たとえば、Microsoft Windows オペレーティングシステム)を使用する多数のコンピュータから成るネットワークで役立ちます。この理由は、ファイアウォールのログファイルは、ブロードキャストによってすぐにいっぱいになるからです。ブロードキャストのドロップルールを手動で定義するには、接続されたすべてのネットワークのブロードキャストアドレスの定義をグループ化し、`255.255.255.255/255.255.255.255`の"global_broadcast"定義を追加し、次にファイアウォール設定上部でこれらのアドレスに対するすべてのトラフィックをドロップするルールを追加します。ブロードキャストを多用するネットワークでは、これによってシステムのパフォーマンスも向上します。
- **IDENTトラフィックのリジェクト:**IDENTリバースプロキシを使用しない場合は、内部ネットワークのポート`113`(IDENT)へのトラフィックをアクティブに拒否できます。これにより、FTP、IRC、および SMTP などの IDENT を使用するサービスの長いタイムアウトを防止できます。

> **Note** – マスカレーディングを使用している場合は、マスカレードされているネットワークに対する IDENT 要求が、マスカレードするインタフェースに届きます。

- NAT はネットワークパケットのアドレスを変更するため、ファイアウォールの機能に影響を与えます。
  - DNAT は*ファイアウォール*の前に適用します。これは、ファイアウォールが、すでに変換されたパケットを「見る」ことを意味します。DNAT 関連のサービスにルールを追加する際は、これを考慮することが必要です。
  - SNAT およびマスカレーディングは*ファイアウォール*の後に適用されます。これは、ファイアウォールは、オリジナルの送信元アドレスを持つ変換されていないパケットをまだ「見る」ことを意味します。

テーブルヘッダのコントロールパネルを使用して、特定の基準でファイアウォールルールをフィルタして、読みやすいようにルールを再構成できます。グループを定義している場合は、ドロップダウンメニューからグループを選択し、このグループに属するすべてのルールを見ることができます。検索フィールドを使用して、キーワードあるいは単に文字列を探して、それに関連するルールを表示できます。検索は、ルールの送信元、宛先、サービス、グループ名、およびコメントで構成されます。

8.1.2 送受信国別ブロック

「*ネットワークプロテクション > ファイアウォール > 送受信国別ブロック*」タブで、特定の国や地域への送受信トラフィックをブロックできます。1つの国や地域あるいは大陸全体をブロックできます。このブロックは、ホストの IP アドレスの GeoIP 情報に基づいています。

送受信国別ブロックを有効にするには、以下の手順に従います。

1. **送受信国別ブロックを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*国*」セクションが編集可能になります。

2. **ブロックする場所を選択します。**
   地域名の前にあるドロップダウンリストで、該当する地域のブロックステータスを指定します。

   - **すべて:**この地域への送受信トラフィックすべてをブロックします。
   - **送信元:**この地域からの受信トラフィックすべてをブロックします。
   - **宛先:**この地域への送信トラフィックすべてをブロックします。
   - **OFF:**この地域との送受信トラフィックを許可します。

ヒント – 特定の大陸にあるすべての地域に対して、同じブロックステータスを容易に指定できます。これには、大陸名の前にあるドロップダウンリストで、必要なブロックステータスを選択します。

3. **「*適用*」をクリックします。**
   設定が保存されます。これで、選択した地域との送受信トラフィックに、指定されたブロックステータスが適用されます。ブロックから除外する地域は、「*国ブロックの例外*」タブで指定できます。

ヒント – このページの各セクションは、セクションヘッダの右にあるアイコンをクリックして、折りたたみ/展開できます。

8.1.3 送受信国除外

「*Network Protection > ファイアウォール > 国ブロックの例外*」タブで、「*送受信国別ブロック*」タブでブロックした国に対する例外を指定できます。送受信方向やトラフィックのサービスに応じて、ブロックした国/地域と特定のホスト/ネットワーク間のトラフィックに対して、例外を指定できます。

国ブロックの例外を作成するには、次の手順に従います。

1. **「*新規除外リスト*」をクリックします。**
   「*除外リストを作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:除外を説明する名前を入力してください。

   コメント(任意):説明などの情報を追加します。

   ブロックしない:

   - **地域:**ドロップダウンリストを使用して、「*国*」ボックスに表示される国を絞り込むことができます。
   - **国:**例外を指定する国や地域の前にあるチェックボックスを選択します。すべての国を一度に選択するには、「*すべて選択*」チェックボックスを選択します。

   すべてのリクエスト:国ブロックから除外する場合の条件を選択します。送信トラフィックや受信トラフィックごとに、対象にするホスト/ネットワークを下部のボックスで指定できます。

   - **ホスト/ネットワーク:**選択したドロップダウンリストのエントリに応じて、指定した国との送信や受信を許可するトラフィックのホスト/ネットワークを追加または選択します。

使用するサービス:選択したホスト/ネットワークと、国/地域の間で許可するサービスを追加します。

3. **「*保存*」をクリックします。**
   国ブロックの例外の最新情報が、「*国ブロックの例外*」リストに表示されます。

除外ルールを編集または削除するには、対応するボタンをクリックします。

8.1.4 ICMP

「*ネットワークプロテクション > ファイアウォール > ICMP*」タブで、*インターネット制御メッセージプロトコル*(ICMP)の設定を構成できます。ICMP を使用して、ホスト間で接続関連のステータス情報をやり取りします。ICMP はネットワーク接続のテストやネットワークの問題のトラブルシューティングに重要です。

このタブで任意の ICMP トラフィックを許可すると、ファイアウォールの ICMP 設定が上書きされます。特定のホストやネットワークだけに ICMP を許可する場合は、「*ファイアウォール > ルール*」タブを使用します。

グローバル ICMP 設定

以下のグローバル ICMP オプションを利用できます。

- **ゲートウェイ上でのICMPを許可:**このオプションで、どの種類の ICMP パケットにもゲートウェイが対応できるようにします。
- **ICMPのゲートウェイ通過を許可:**このオプションを使用すると、パケットが内部ネットワーク、つまりデフォルトゲートウェイを使用しないネットワークから送信される場合、すべての ICMP パケットをゲートウェイを通して転送可能になります。
- **ICMPリダイレクトをログ:**ICMP リダイレクトは、パケットの宛先へのより良いルートを探すために、1台のルータから別のルータに送信されます。ルータはルーティングテーブルを変更して、より適切と想定されるルートを経由して同じ宛先にパケットを送ります。このオプションを選択すると、ゲートウェイが受信したすべての ICMP リダイレクトがファイアウォールログにログされます。

ping 設定

ping プログラムは、IP ネットワークを横断して特定ホストに到達できるかどうかをテストするためのコンピュータネットワークツールです。ping は、ICMP *エコー要求*パケットをターゲットホストに送信し、ICMP *エコー応答*による返信を待機することで機能します。ping は、間隔のタイミングと応答率を使用して、ホスト間の往復時間とパケット紛失率を評価します。

以下の ping オプションを利用できます。

- **ゲートウェイは ping で可視:**ゲートウェイは ICMP *エコー要求*パケットに応答します。この機能はデフォルトで有効になっています。
- **ゲートウェイからの ping:**ゲートウェイで ping コマンドを使用できます。この機能はデフォルトで有効になっています。
- **ゲートウェイは ping を転送:**ゲートウェイは、内部ネットワーク、つまりデフォルトゲートウェイを使用しないネットワークから送信される ICMP *エコー要求*および*エコー応答*パケットを転送します。

Traceroute設定

traceroute(トレースルート)プログラムは、IP ネットワーク上でパケットが使用するルートの決定に使用されるコンピュータネットワークツールです。traceroute は、パケットの伝送に関与したルータの IP アドレスを一覧表示します。一定の時間内にパケットのルートを判断できない場合は、IP アドレスの代わりにアスタリスク(*)で報告します。一定の回数だけ失敗すると、確認作業は終了します。確認の中断には多くの理由が考えられますが、ほとんどの場合は、ネットワークパスのファイアウォールが traceroute パケットをブロックすることが原因となります。

以下の traceroute オプションを利用できます。

- **ゲートウェイは traceroute で可視:**ゲートウェイは traceroute パケットに応答します。
- **ゲートウェイは traceroute を転送:**ゲートウェイは 内部ネットワーク、つまりデフォルトゲートウェイを使用しないネットワークから送信される traceroute を転送します。

注 – さらに、UNIX traceroute アプリケーション用の UDP ポートも開きます。

8.1.5 詳細

「*ネットワークプロテクション > ファイアウォール > 詳細*」タブには、ファイアウォールおよび NAT ルールの詳細設定が含まれています。

コネクショントラッキングヘルパ

コネクショントラッキングヘルパを使用することにより、複数のネットワークコネクションを使用するプロトコルでファイアウォールあるいはNATルールを使用できます。ファイアウォールが取り扱うすべての接続は、*conntrack* カーネルモジュール(*コネクショントラッキング*プロセスとも呼ばれます)で追跡します。FTP や IRC などのプロトコルにはいくつかのポートを開くことが必要で、それらの正常な機能をサポートする特別なコネクショントラッキングヘルパが必要になります。これらのヘルパは特別なカーネルモジュールで、追加の接続をそれらを最初の接続に関連付けることによって(通常はデータストリームから関連するアドレスを読み取ることで)特定します。

たとえば、FTP の接続が正常に機能するには、FTP conntrack ヘルパを選択する必要があります。これは FTP プロトコルの特異性によるもので、それによって FTP コントロールコネクションと呼ばれる単一の接続を確立します。この接続でコマンドが発行されると、他のポートが開いてその特定コマンドに関連するデータの残りを実行します(例: ダウンロードあるいはアップロード)。問題は、それらは動的にネゴシエートされたため、ゲートウェイがこれらの特別なポートを知らない、ということです。したがって、ゲートウェイは、これらの特定のポートでサーバをクライアントに接続させなければならないか(アクティブな FTP 接続)、またはインターネット上でクライアントを FTP サーバに接続させなければならないか(パッシブな FTP 接続)を知ることができません。

これが FTP conntrack ヘルパが役に立つ理由です。この特別なヘルパは特別なコネクショントラッキングモジュールに追加され、特別な情報の制御接続(通常はポート21)をスキャンします。ヘルパが正しい情報に出会うと、その情報をコントロールコネクションの関連情報として想定される接続のリストに追加します。これにより、ゲートウェイで最初の FTP コネクションと関連する全コネクションの両方を追跡することが可能になります。

コネクショントラッキングヘルパは以下のプロトコルで使用できます。

- FTP
- IRC(DCC用)
- PPTP
- TFTP

注 – ファイアウォールで PPTP VPN サービスを提供したい場合は、PPTP ヘルパモジュールをロードする必要があります。ロードしないと、PPTPセッションは確立できません。この理由は、PPTP は、別個の IP プロトコルの *Generic Routing Encapsulation*(GRE)通信に切り換える前に、TCP ポート 1723 接続を確立するからです。PPTP ヘルパモジュールをロードしないと、すべての GRE パケットはゲートウェイにブロックされます。PPTP ヘルパモジュールを使用しない場合は、代わりにファイアウォールルールを手動で追加し、受信および送信トラフィックで GRE パケットを許可します。

プロトコル処理

TCP ウィンドウスケーリングの有効化:TCP の受信ウインドウ(RWin)サイズは、接続時にバッファできる受信データ量(バイト単位)です。送信側ホストは、受信側ホストからの受信確認とウィンドウの更新を待つ間、その量のデータのみを送信できます。高帯域幅ネットワークをさらに効率的に使用するために、大きな TCP ウインドウサイズを使用できます。ただし、TCP ウインドウサイズのフィールドはデータの流れを制御し、2バイトあるいは 65535バイトのウインドウサイズに制限されています。サイズフィールドは拡張できないため、スケーリングファクタを使用します。TCP ウインドウのスケーリングは TCP/IP スタックのカーネルオプションで、最大ウインドウサイズを 65535バイトか

ら 1ギガバイトに拡大するために使用できます。デフォルトではウインドウスケーリングが有効になっています。しかし、ルータ、ロードバランサ、ゲートウェイなどの一部のネットワークデバイスはウインドウのスケーリングをまだ完全にはサポートしていないため、環境によってはスケーリングをオフにすることが必要な場合があります。

厳密な TCP セッション処理を使用:デフォルトでは、システムはネットワーク機能のリセットにより、コネクショントラッキングテーブルで現在扱われていない既存の TCP 接続を抽出できます。これは SSH および Telnet などの対話型セッションが、ネットワークインタフェースが一時的に利用できない場合に停止しないことを意味します。このオプションを有効にすると、そのようなセッションを再度確立するには新しい 3WAY ハンドシェークが常に必要になります。一般的にはこのオプションはオフのままにしておくことをお勧めしています。

パケット長の有効性を確認:有効にすると、ファイアウォールは、ICMP、TCP、または UDP プロトコルの使用時に、データパケットが最小長を満たしているかチェックします。データパケットが最小値より小さい場合、それらはブロックされ、その記録がファイアウォールログに書き込まれます。

Spoof(なりすまし)防御:デフォルトで、なりすまし保護は無効になっています。以下の設定から選択できます。

- **通常:**ゲートウェイは、インタフェース自体と同じ送信元 IP アドレスを持つパケット、またはそのインタフェースに別に割り当てられたネットワークの送信元IPを持つインタフェースに到着するパケットを、ドロップしてログします。
- **厳密:**ゲートウェイは、宛先 IP にインタフェースが指定され、割り当てられた以外のインタフェースに到着する(つまり、宛先として指定されていないインタフェースに到着する)すべてのパケットをドロップしてログします。たとえば、内部ネットワークのみからパケットを受け付けると想定される内部インタフェースの IP アドレスに外部ネットワークから送信されたパケットはドロップされます。

ログオプション

FTPデータコネクションのログ:UTM は、ファイルおよびディレクトリー覧の FTP データ接続をログします。ログレコードには「FTP data (FTP データ)」という文字列によってマークが付けられます。

ユニークな DNS リクエストのログ:UTM は、DNS サーバへのすべての要求およびそれらの結果をログします。ログレコードには「DNS request」という文字列によってマークが付けられます。

破棄したブロードキャストのログ: デフォルトでは、ファイアウォールはすべてのブロードキャストを破棄し、ログも行いません。しかし、たとえば監査のためにブロードキャストをファイアウォールログに記録する必要がある場合は、このオプションを選択します。

8.2 NAT

「*ネットワークプロテクション > NAT*」メニューを使用すると、ゲートウェイの NAT ルールを定義し、管理することができます。*ネットワークアドレス変換*(NAT)とは、ルータやゲートウェイを通過する IP パケットの送信元アドレスまたは宛先アドレス あるいは両方)を書き換えるプロセスです。NAT を使用するほとんどのシステムは、プライベートネットワーク上の複数のホストが 1つのパブリック IP アドレスを使用してインターネットにアクセスできるようにするために NAT を使用しています。あるクライアントが IP パケットをルータに送信すると、NAT は送信アドレスを別のパブリック IP アドレスに変換してからインターネットにパケットを転送します。応答パケットを受信すると、NAT はパブリックアドレスを元のアドレスに変換し、クライアントにパケットを転送します。システムリソースに応じて、NAT は自己裁量で大規模内部ネットワークに対応できます。

8.2.1 マスカレード

マスカレードとは、*送信元ネットワークアドレス変換*(SNAT)の特殊ケースであり、ネットワークインタフェース(通常は、インターネットに接続された外部インタフェース)上の 1つの公式 IP アドレスの背後に内部ネットワーク(通常はプライベートアドレススペースを持つ LAN)をマスカレードすることができます。SNAT の場合、複数の送信元アドレスを複数の宛先アドレスにマッピングすることができるため、より汎用的です。

注 – 送信元アドレスは、指定されたインタフェース経由でパケットがゲートウェイシステムから配信された場合にのみ変換されます。新しい送信元アドレスは常に、当該インタフェースの最新IP アドレスとなります(つまり、このアドレスは動的です)。

マスカレードルールを作成するには、次の手順に従います。

1. **「*マスカレード*」タブで「*新規マスカレードルール*」をクリックします。**
   「*新規マスカレードルールの作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   ネットワーク:マスカレードする(内部)ネットワークを選択します。

   I/F(インタフェース):インターネットに接続する(外部)インタフェースを選択します。

   使用するアドレス:選択したインタフェースに複数の IP アドレスが割り当てられている場合(「*インタフェースとルーティング > インタフェース > 追加アドレス*」を参照)、マスカレードに使用する IP アドレスをここで定義できます。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しいマスカレードルールが *マスカレード*ルールのリストに表示されます。
4. **マスカレードルールを有効にします。**
   マスカレードルールを有効にするには、トグルスイッチをクリックします。

ルールを編集または削除するには、対応するボタンをクリックします。

注 – クライアントが外部サーバにアクセスできるようにするには、ファイアウォールで内部ネットワークからインターネットへのトラフィックを許可する必要があります。

IPsec パケットはマスカレードルールの影響を受けません。IPsec パケットの送信元アドレスを変換するには、SNAT またはフル NAT ルールを作成します。

8.2.2 NAT

DNAT *(Destination Network Address Translation)* と SNAT *(Source Network Address Translation)* は、いずれも NAT の特殊ケースです。SNAT では、接続を開始したコンピュータの IP アドレスが書き換えられます。一方、DNAT では、データパケットの宛先アドレスが書き換えられます。DNAT は、内部ネットワークでプライベート IP アドレスを使用しており、管理者が一部のサービスを外部からも使用可能にしたい場合に特に便利です。

これは、例を使って説明するとわかりやすいでしょう。内部ネットワークでアドレススペース `192.168.0.0/255.255.255.0` を使用しており、Web サーバが IP アドレス `192.168.0.20` で機能しているとします。この場合、インターネット経由のクライアントに対してポート `80` を使用可能にする必要があります。`192.168`.アドレススペースはプライベートであるため、インターネット経由のクライアントはWeb サーバにパケットを直接送信できません。ただし、UTMの外部(公開)アドレスと通信することはできます。この場合、DNAT は、システムアドレスのポート`80` 向けのパケットを捕捉し、内部 Web サーバに転送できます。

注 – *PPTP VPN アクセス*は DNAT に対応していません。

常にプライマリネットワークインタフェースアドレスにマッピングするマスカレードと異なり、SNAT は送信元アドレスを SNAT ルールに指定されたアドレスにマッピングします。

1:1 NAT は DNAT または SNAT の特殊なケースです。この場合、ネットワーク全体のすべてのアドレスが同じネットマスクを持つ別のネットワークのアドレスに 1 対 1 で変換されます。したがって、元のネットワークの最初のアドレスが他のネットワークの最初のアドレスに変換され、元のネット

ワークの 2番目のアドレスが他のネットワークの 2番目のアドレスに変換されるという様になります。1:1 の NAT ルールは、送信元アドレスまたは宛先アドレスに適用することができます。

注 – デフォルトで、ポート443(HTTPS)はユーザポータルに使用されます。ポート443を内部サーバに転送する予定がある場合、「*マネジメント > ユーザポータル > 詳細*」タブでユーザポータルの TCP ポートを他の値(1443など)に変更する必要があります。

DNAT はファイアウォールの前に行われるため、適切なファイアウォールルールを定義しておく必要があります。詳しくは、「*ネットワークプロテクション > ファイアウォール > ルール*」を参照してください。

NAT ルールを定義するには、次の手順に従います。

1. **「*NAT*」タブで、「*新規 NAT ルール*」をクリックします。**
   「*新規 NAT ルールの作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   グループ:「*グループ*」オプションは、複数のルールを論理的にグループ化するのに便利です。リストの上部のドロップダウンリストを使用して、グループごとにルールをフィルタリング表示できます。グループ化は表示用のみで、ルールの一致には関係ありません。新しいグループを作成するには、「*<< 新規グループ >>*」エントリを選択し、グループを説明する名前を「*名前*」に入力します。

   優先順位:優先順位番号。これによってルールの優先順位が定義されます。番号が小さいほど優先順位が高くなります。ルールは昇順に照合されます。あるルールが一致すると、それ以降、それより大きい番号のルールは評価されません。

   ルールタイプ:ネットワークアドレス変換モードを選択します。選択に応じて、さまざまなオプションが表示されます。次のモードを使用できます。

   - **SNAT(送信元):**定義された IP パケットの送信元アドレスを 1つの新しい送信元アドレスにマッピングします。サービスを変更することもできます。
   - **DNAT(宛先):**定義された IP パケットの宛先アドレスを 1つの新しい宛先アドレスにマッピングします。サービスを変更することもできます。
   - **1:1 NAT(ネットワーク全体):**ネットワークの IP アドレスを別のネットワークに1対1でマッピングします。このルールは、定義された IP パケットの送信元アドレスか宛先アドレスに適用されます。

- **フル NAT(送信元＋宛先):**定義された IP パケットの送信元アドレスと宛先アドレスの両方を1つの新しい送信元アドレスと1つの新しい宛先アドレスにマッピングします。送信元サービスとターゲットサービスを変更することもできます。
- **NAT除外:**このオプションは例外ルールの一種と考えることができます。たとえば、定義したネットワークに NAT ルールがある場合、このネットワーク内の特定のホストに対して「*NAT除外*」ルールを作成することができます。これにより、これらのホストは NAT の対象外となります。

マッチング条件:送信元および宛先ネットワーク/ホストとアドレスを変換するサービスを選択します。

- **トラフィック送信元:**パケットの元の送信元アドレス。1つのホストにすることも、ネットワーク全体にすることもできます。
- **サービス:**パケットのオリジナルのサービスタイプ(送信元ポートと宛先ポート、およびプロトコルタイプから構成されています)。

  注 – トラフィックサービスは、対応するアドレスも変換される場合のみ変換できます。さらに、2つのサービスが同じプロトコルが使用する場合のみ、サービスを別のサービスに変換できます。

- **トラフィック宛先:**パケットの元の宛先アドレス。1つのホストにすることも、ネットワーク全体にすることもできます。

アクション:送信元/宛先、元の IP パケットデータを変換するサービスタイプを選択します。表示されるパラメータは選択されている「*ルールタイプ*」に依存します。

- **変更後の送信元**(「*SNAT*」または「*フル NAT*」モードのみ):送信元ホスト、つまりパケットの新しい送信元アドレスを選択します。
- **変換後の送信元**(「*DNAT*」または「*フル NAT*」モードのみ):宛先ホスト、つまりパケットの新しい宛先アドレスを選択します。
- **変更後のサービス**(「*DNAT*」、「*SNAT*」、または「*フル NAT*」モードのみ):パケットの新しいサービスを選択します。選択されている「*ルールタイプ*」によっては、送信元/宛先サービスとすることができます。
- **1:1 NATモード**(「*1:1 NAT*」モードのみ):次のモードのいずれかを選択します。
  - **マップ宛先:**宛先アドレスを変更します。
  - **マップ送信元:**送信元アドレスを変更します。

> **注 –** 送信元をマッピングする場合は、「*トラフィック送信元*」フィールドにネットワーク全体を追加し、宛先をマッピングする場合は「*トラフィック宛先*」フィールドにネットワーク全体を追加する必要があります。

- **マップ先**(「*1:1 NAT*」モードのみ):元の IP アドレスの変換先となるネットワークを選択します。元のネットワークと変換先のネットワークが同じネットマスクである必要があります。

自動ファイアウォールルール(任意):該当するトラフィックがファイアウォールを通過することを許可するファイアウォールルールを自動的に生成する場合に、このオプションを選択します。

コメント(任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   IPsec パケットにルールを適用(「*SNAT*」または「*フル NAT*」モードのみ):IPsec で処理するトラフィックにルールを適用する場合にこのオプションを選択します。デフォルトではこのオプションが選択されていないため、IPsec トラフィックが SNAT から除外されることになります。

   初期パケットのログ(任意):このオプションは、通信の初期化パケットをファイアウォールログに書き込む場合に選択します。これにより、NAT ルールを使用する場合はいつでも、ファイアウォールログに「NAT を使用する接続(Connection using NAT)」というメッセージが記述されます。このオプションは、ステートフルプロトコルでもステートレスプロトコルでも機能します。

4. **「*保存*」をクリックします。**
   新しいルールが「*NAT*」リストに表示されます。

5. **NAT ルールを有効にします。**
   新しいルールはデフォルトで無効になっています(トグルスイッチはグレー表示)。ルールを有効にするには、トグルスイッチをクリックします。

ルールを編集または削除するには、対応するボタンをクリックします。

8.3 侵入防御(IPS)

「*ネットワークプロテクション > 侵入防御*」メニューで、ゲートウェイの IPS ルールを定義し、管理することができます。侵入防御システム(IPS)は、シグニチャに基づく *IPS* ルールセットを利用して攻撃を認識します。システムは、トラフィックを完全に分析し、ネットワークに到達する前に攻撃を自動的にブロックします。既存のルールセットと攻撃パターンは、パターン更新によって最新状態に更

新されます。新しい IPS 攻撃パターンのシグニチャは、IPS ルールとしてルールセットに自動的にインポートされます。

8.3.1 グローバル

「*ネットワークプロテクション > 侵入防御 > グローバル*」タブでは、Sophos UTMの*侵入防御システム*(IPS)を有効にすることができます。

IPSを有効にするには、次の手順に従います。

1. **侵入防御システムを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*グローバル IPS設定*」エリアが編集可能になります。

2. **次の設定を行います。**
   ローカルネットワーク:侵入防御システムで防御するネットワークを選択します。ローカルネットワークを選択しないと、侵入防御は自動的に無効になり、トラフィックはモニタリングされません。

   ポリシー:ブロッキングルールが IPS 攻撃シグネチャを検出したときに侵入防御システムが使用するセキュリティポリシーを選択します。

   - **破棄:**データパケットは、他のアクションなしで破棄されます。
   - **接続を終了:**終了データパケット(*TCP* の場合は RST、UDP 接続の場合は *ICMP Port Unreachable*)が両方の通信パートナーに送信され、接続が終了します。

   注 – デフォルトでは「*破棄*」が選択されています。通常はこの設定を変更する必要はありません。これは特に、疑わしい侵入者に中止データパケットが悪用され、ゲートウェイについての情報が引き出されてしまう可能性があるためです。

3. **「*適用*」をクリックします。**
   設定が保存されます。

ライブログ

侵入防御ライブログは、選択した IPS ルールのモニタリングに使用できます。ボタンをクリックして、新しいウィンドウでライブログを開きます。

8.3.2 攻撃パターン

「*ネットワークプロテクション > 侵入防御 > 攻撃パターン*」タブには、共通の攻撃パターンに従ってグループ分けされたIPSルールが表示されます。攻撃パターンは次のようにまとめられています。

- **OS固有の攻撃:**OS関連の脆弱性を悪用しようとする攻撃。
- **サーバに対する攻撃:**Webサーバ、メールサーバなどあらゆる種類のサーバを対象とする攻撃。
- **クライアントソフトウェアに対する攻撃:**Webブラウザ、マルチメディアプレーヤなどのクライアントソフトウェアを対象とする攻撃。
- **プロトコルアノマリー:**ネットワークの異常を探す攻撃パターン。
- **マルウェア:**所有者の許可なしで、コンピュータシステムへの侵入や破壊を行うように設計されたソフトウェア(トロイの木馬、DoS通信ツールなど)。

パフォーマンス向上のために、会社のローカルネットワークに導入されているサービスまたはソフトウェアに該当しないチェックボックスはチェックを外してください。たとえば、ローカルネットワーク内でWebサーバを運用していない場合は、「*HTTP サーバ*」用の選択を取り消すことができます。

各グループに対して、次の設定を使用できます。

アクション:デフォルトで、グループ内の各ルールにはアクションが関連付けられています。次のアクションを選択できます。

- **破棄:**デフォルト設定。攻撃の疑いがある試行が見つかると、その原因であるデータパケットはドロップされます。
- **警告:**「*破棄*」設定と異なり、重大なデータパケットはゲートウェイを通過できますが、IPSログに警告メッセージが作成されます。

注 – 個々のIPSルールの設定を変更するには、「*侵入防御 > 詳細*」タブの「*変更されたルール*」ボックスを使用します。Sophos UTM 9で使用されているIPSルールの詳細なリストは、UTM Webサイトを参照してください。

追加の警告ルールを有効化:このオプションを選択すると、各グループにルールが追加され、IPS検出率が向上します。これらのルールは、明示的な攻撃パターンよりも一般的で曖昧なので、アラートの数が増える可能性があります。このため、これらのルールのデフォルトアクションは「*警告*」であり、設定はできません。

通知:このオプションを選択すると、このグループと一致するIPSイベントが発生するたびに管理者に通知が送信されます。このオプションが有効になるのは、「*マネジメント > 通知 > 通知*」タブで侵入防御システムの通知機能を有効にした場合のみです。さらに、送信される通知のタイプ(つまり、メールまたはSNMPトラップ)は、ここでの設定によって決まります。また、通知設定の変更が有効になるまでは最大5分かかる場合があります。

8.3.3 DoS/フラッド防御

「*DoS/フラッド防御*」タブでは、DoS(*サービス拒否*)攻撃とDDoS(*分散型サービス拒否*)攻撃から防御するためのオプションを設定できます。

一般にDoS攻撃とDDoS攻撃は、正当な要求がコンピュータリソースを使用できないようにします。シンプルな例では、攻撃者はサーバに無意味なパケットを送信して過負荷をかけ、パフォーマンスに負担をかけます。このような攻撃には大規模な帯域幅が必要となるため、いわゆる*SYNフラッド攻撃*を使用する攻撃者が増え続けています。この攻撃は、帯域幅の過負荷ではなく、システムリソースのブロックを目的としています。この目的のために、攻撃者は多くの場合、偽造された送信元アドレスを使用してサービスのTCPポートにSYNパケットを送信します。これに対し、サーバはTCP/SYN-ACKを送り返して、これに応答する送信元アドレスからのTCP/ACKパケットを待ち続けるため、接続がhalf-open状態になります。ところが、送信元アドレスは偽造されているため、応答は返ってきません。これらのhalf-open状態の接続により、サーバが対応できる接続数が飽和状態になり、正当な要求に対応できなくなります。

このような攻撃は、特定時間内にネットワークに対して送信されるSYN(TCP)、UDP、ICMPパケットの数を制限することで回避できます。

TCP SYN フラッド防御

SYN(TCP)フラッド防御を有効にするには、次の手順に従います。

1. **「*DoS/フラッド防御*」タブで、「*TCP SYN フラッド防御の使用*」チェックボックスにチェックを入れます。**
2. **次の設定を行います。**
   モード:次のモードを使用できます。
   - **送信元及び宛先アドレス:**送信元IPアドレスと宛先IPアドレスの両方と一致するSYNパケットを破棄する場合、このオプションを選択します。まず、送信元IPアドレスに一致するSYNパケットは、以下で指定する送信元パケットレートの値で制限されます。次に、要求がまだ多すぎる場合には、宛先IPアドレスに基づいて追加でフィルタリングされ、また、以下で指定する宛先パケットレートの値で制限されます。このモードはデフォルトで設定されています。

- **宛先アドレスのみ:**宛先 IP アドレスのみに従って SYN パケットを破棄する場合、このオプションを選択します。
- **送信元アドレスのみ:**送信元 IP アドレスのみに従って SYN パケットを破棄する場合、このオプションを選択します。

ログ:このオプションを使用すると、ログレベルを選択できます。以下のレベルを設定できます。

- **OFF:**ログを完全にオフにする場合、このログレベルを選択します。
- **制限:**ログを 1秒あたり 5パケットに制限する場合、このログレベルを選択します。デフォルトではこのレベルが設定されています。
- **すべて:**すべての SYN (TCP) 接続試行を詳細にログする場合、このログレベルを選択します。SYN (TCP) フラッド攻撃により、ログが膨大になる可能性があります。

送信元パケットレート:ここに、送信元 IP アドレスに対して許可される 1秒あたりのパケットレートを指定できます。

宛先パケットレート:ここに、宛先 IP アドレスに対して許可される 1秒あたりのパケットレートを指定できます。

注 – ここで合理的な値を入力することは重要です。レートを高く設定し過ぎると、Web サーバがそのように大量な SYN (TCP) パケットに対処しきれず、障害が発生する可能性などがあります。一方、レートを低く設定し過ぎると、ゲートウェイが通常の SYN (TCP) 要求をブロックして、予期しない挙動をする可能性があります。各システムの合理的な設定は、ハードウェアに大きく依存します。従って、システムに適した値にデフォルト値を置き換えてください。

3. **「*適用*」をクリックします。**
   設定が保存されます。

UDP フラッド防御:

*UDP フラッド防御*機能は、UDP パケットフラッドを検出し、ブロックします。
「*UDP フラッド防御*」の設定は、「*TCP SYN フラッド防御*」の設定と同じです。

ICMP フラッド防御:

*ICMP フラッド防御*機能は、ICMP パケットフラッドを検出し、ブロックします。
「*ICMP フラッド防御*」の設定は、「*TCP SYN フラッド防御*」の設定と同じです。

8.3.4 ポートスキャン防御

「*ネットワークプロテクション > 侵入防御 > ポートスキャン防御*」タブでは、一般的なポートスキャン検知オプションを設定することができます。

ポートスキャンとは、セキュアなシステムで使用可能なサービスを探るためにハッカーが用いる手段です。システムに侵入したり、DoS 攻撃を開始したりするために、攻撃者はネットワークサービスに関する情報が必要です。このような情報を入手すると、攻撃者はこれらのサービスにあるセキュリティ上の欠陥を悪用しようとします。インターネットプロトコル TCP および UDP を使用しているネットワークサービスは、特別なポートからアクセス可能であり、このポート割り当ては一般によく知られています。たとえば、SMTP サービスは TCP ポート 25 に割り当てられています。サービスで使用されるポートは、オープンであると見なされます。これは、このようなポートへの接続を確立することができるためです。一方、使用されていないポートはクローズと見なされ、これらのポートへの接続を試みると失敗します。攻撃者は、ポートスキャナという特別なソフトウェアツールを利用してオープンポートを探します。このプログラムは、攻撃対象のコンピュータ上にある複数のポートに対して接続を試みます。接続が成功したポートはオープンであるとツールに表示されます。こうして攻撃者は、攻撃対象のコンピュータにおいてどのネットワークサービスが使用可能であるかを示す必要な情報を入手します。

インターネットプロトコル TCP と UDP では、使用可能なポートが全部で 65535個あるため、ポートは非常に短い間隔でスキャンされます。サービスへ接続しようとする試行が異常に大量に発生していることをゲートウェイが検出した場合 (特に、これらの試行が同じ送信元アドレスから送信されている場合)、ゲートウェイがポートスキャンを受けている可能性が高くなります。攻撃者の疑いのある人がネットワーク上のホストまたはサービスのスキャンを行うと、ポートスキャン検出機能がこれを認識します。オプションで、同じ送信元アドレスから繰り返されるポートスキャンを自動的にブロックすることができます。ポートスキャン検知は、インターネットインタフェース、つまりデフォルトゲートウェイを装備したインタフェースに制限されています。

技術的に言うと、ポートスキャンが検出されるのは、1つの送信元 IP アドレスの検出スコアが 300ミリ秒の時間枠内で 21点を超えたときです。検出スコアは次のように計算されます。

- 1024 未満の TCP 宛先ポートに対するスキャン = 3点
- 1024 以上の TCP 宛先ポートに対するスキャン = 1点

ポートスキャン検出を有効するには、次の手順に従ってください。

1. **「*ポートスキャン防御*」タブで、「*ポートスキャン検知*」を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、「*グローバル設定*」エリアが編集可能になります。

2. **次の設定を行います。**
   アクション:次の作業を実行できます。

   - **ログイベントのみ:**ポートスキャンに対する対策は行われません。イベントのログが記録されるだけです。
   - **トラフィックを破棄:**さらなるポートスキャンパケットは、ユーザに通知することなく破棄されます。ポートスキャナは、これらのポートがフィルタされたことを報告します。
   - **トラフィックを拒否:**さらなるポートスキャンパケットは破棄され、ICMP「destination unreachable/port unreachable(宛先到達不可/ポート到達不可)」応答が送信者に送られます。ポートスキャナは、これらのポートがクローズされたことを報告します。

   ログを制限:ログメッセージの数を抑えたい場合に、このオプションを有効にします。ポートスキャン検出機能は、ポートスキャンが実行されているときに大量のログを生成します。たとえば、ポートスキャンに使用されていると見なされるそれぞれの SYN パケットに対して、ファイアウォールログにエントリが 1つ生成されます。このオプションを選択すると、ログが 1秒あたり 5行までに制限されます。

3. **「*適用*」をクリックします。**
   設定が保存されます。

8.3.5 除外

「*ネットワークプロテクション > 侵入防御 > 除外*」タブでは、侵入防御から除外する送信元ネットワークと宛先ネットワークを定義することができます。

除外ルールを作成するには、次の手順に従います。

1. **「*除外*」タブで、「*新規除外リスト*」をクリックします。**
   「*除外リストを作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:この除外ルールを説明する名前を入力してください。

   スキップするチェック:スキップするセキュリティチェックを選択します。

   - **侵入防御(IPS):**このオプションを選択すると、Sophos UTM の IPS が無効になります。
   - **ポートスキャン防御:**このオプションを選択すると、ネットワークホストでオープンポートを探すことを目的とする攻撃からの防御が無効になります。
   - **TCP SYN フラッド防御:**選択すると、TCPSYN フラッド攻撃からの防御が無効になります。

- **UDP フラッド防御:**選択すると、UDP フラッド攻撃からの防御が無効になります。
- **ICMP フラッド防御:**選択すると、ICMP フラッド攻撃からの防御が無効になります。

対象:セキュリティチェックをスキップする条件を少なくとも 1つ選択します。条件の前にあるドロップダウンリストで「*And*」または「*Or*」を選択して、複数の条件を論理的に組み合わせることができます。次の条件を設定できます。

- **送信元ネットワーク:**選択して、この例外ルールのセキュリティチェックから除外する送信元ホスト/ネットワークを追加します。条件を選択後、表示される「*ネットワーク*」ボックスに各ホストやネットワークを入力します。
- **使用するサービス:**選択して、この例外ルールのセキュリティチェックから除外する送信元ホスト/ネットワークを追加します。条件を選択後、表示される「*サービス*」ボックスに各サービスを追加します。
- **宛先:**選択して、この例外ルールのセキュリティチェックから除外するホスト/ネットワークを追加します。条件を選択後、表示される「*宛先*」ボックスに各ホストやネットワークを入力します。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しい除外が「*除外*」リストに表示されます。
4. **除外リストを有効にします。**
   新しい除外はデフォルトで無効になっています(トグルスイッチはグレー表示)。例外を有効にするには、トグルスイッチをクリックします。

   これで除外リストが有効になります(トグルスイッチは緑色)。

除外ルールを編集または削除するには、対応するボタンをクリックします。

注 – ゲートウェイの宛先アドレスを持つパケットに対する侵入防御を除外したい場合、「*宛先*」ボックスで、「すべて」を選択すると成功しません。ゲートウェイの内部アドレスに対する侵入防御を除外したい場合には、代わりに、「*内部 (アドレス)*」など、ゲートウェイの IP アドレスが含まれるゲートウェイのインタフェース定義を選択する必要があります。また、プロキシ使用時に特定の宛先に対するトラフィックを除外したい場合(HTTPプロキシ使用時の特定のWebサーバ宛てなど)、送信元にプロキシが使用するゲートウェイのインタフェースアドレス定義を指定する必要があります。

8.3.6 詳細

「*ネットワークプロテクション > 侵入防御 > 詳細*」タブでは、各 IPS ルールを手動で変更し、攻撃パターングループから取得されるデフォルトポリシーを上書きできます。熟練ユーザのみが設定してください。

変更したルールを作成するには、次の手順に従います。

1. **「*変更されたルール*」ボックスで、「+」アイコンをクリックします。**
   「*ルールの変更*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   ルールID:変更するルールの ID を入力します。ルール ID を検索するには、Sophos Web サイトの IPS ルールのリストを参照してください。(フォルダで、名前に *IPS-rules* のあるファイルを参照してください。HTML 形式と XML 形式の両方が用意されており、UTM の各バージョンや各パターンバージョン用のファイルがあります。)さらに、IPS ログまたは IPS レポートでも決定できます。

   このルールを無効化:このオプションを選択すると、該当する ID のルールが無効になります。

   選択*しない*場合、次の 2つのオプションを使用できます。

   - **通知の無効化:**このオプションを選択すると、当該ルールが適用された場合に通知が送信されません。
   - **アクション:**各ルールが関連付けられるアクション。次のアクションを選択できます。
     - **破棄:**攻撃の疑いがある試行が見つかると、その原因であるデータパケットはドロップされます。
     - **警告:**「*破棄*」設定と異なり、重大なデータパケットはゲートウェイを通過できますが、IPS ログに警告メッセージが作成されます。

3. **「*保存*」をクリックします。**
   「*変更されたルール*」ボックスにルールが表示されます。変更を確定するためには、ページの一番下にある「*適用*」をクリックする必要もあります。

注–「*変更されたルール*」ボックスにルール ID を追加し、アクションを「*警告*」に設定した場合、この変更が有効になるのは、ルールが属するグループが「*攻撃パターン*」タブで有効になっている場合のみです。該当する攻撃パターングループが無効になっている場合、各 IPS ルールへの変更は効果がありません。

パフォーマンスチューニング

さらに、侵入防御システムのパフォーマンスを向上し、誤検出による警告を最低限に抑えるために、IPS ルールの範囲を内部サーバの一部に制限することができます。たとえば、「*攻撃パターン*」タブで「*HTTP サーバ*」を有効にし、特定の HTTP サーバをここで選択したとします。この場合、侵入防御システムが HTTP サーバへの攻撃を認識しても、関連付けられたアクション(「*ドロップ*」または「*アラート*」)は、影響を受けるサーバの IP アドレスとここで選択された HTTP サーバの IP アドレスが一致する場合に限り、適用されます。

次のサーバタイプに対して、IPS ルールの範囲を制限できます。

- **HTTP:***HTTP サーバ*に含まれているすべての攻撃パターングループ
- **DNS:**攻撃パターングループ *DNS*
- **SMTP:**攻撃パターングループ *Exchange* および *Sendmail*
- **SQL:**データベースサーバに含まれているすべての攻撃パターングループ

8.4 サーバロードバランシング

サーバロードバランシング機能により、受信接続(例: SMTP または HTTP トラフィック)をゲートウェイの背後の複数サーバに分散できます。負荷分散は、送信元 IP アドレスに基づいて、1時間持続して行われます。同じ送信元 IP アドレスから送信された 2つの要求の間隔がこの持続時間を上回ると、バランシングは再決定されます。トラフィックの分散は単純なラウンドロビンアルゴリズムに基づいています。

サーバプールのすべてのサーバは ICMP ping、TCP 接続の確立、または HTTP/S 要求により監視されます。障害が発生すると、影響を受けたサーバは負荷分散に使用されなくなり、問題と考えられる送信元 IP の持続性は却下されます。

注 – HTTP/S 要求のリターンコードは `1xx Informational`、`2xx Success`、`3xx Redirection`、または `4xx Client Error` のいずれかであることが必要です。その他のすべてのリターンコードは障害の発生を意味します。

8.4.1 分散ルール

「*ネットワークプロテクション > サーバロードバランシング > 負荷分散ルール*」タブで、Sophos UTM ソフトウェアの負荷分散ルールを作成できます。ルールの作成後、サーバ間での重み分散を追加で定義し、インタフェースパーシスタンスを設定することができます。

負荷分散のルールを作成するには、以下の手順に従います。

1. **「*負荷分散ルール*」タブで、「*新規負荷分散ルール*」をクリックします。**
「*新規負荷分散ルールの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
サービス:負荷分散するネットワークサービスを選択します。

仮想サーバ:受信トラフィックの元のターゲットホスト。このアドレスは通常、ゲートウェイの外部アドレスと同じになります。

バックエンドサーバ:代わりにサービスのトラフィックを受け付けるホスト。

チェック対象:サービスのモニタリング用に「*TCP*」(TCP 接続の確立)、「*UDP*」(UDP 接続の確立)、「*Ping*」(ICMP Ping)、「*HTTP ホスト*」(HTTP 要求)、または「*HTTPS ホスト*」(HTTPS 要求)のいずれかを選択します。「*UDP*」を使用する場合、ping 要求が最初に送信され、成功した場合は、続いてペイロード 0 の UDP パケットが送信されます。ping が成功しなかった場合や、ICMP ポートに到達できない場合、このサーバはダウンしているとみなされます。*HTTP* および *HTTPS* 要求の場合は、「*URL*」を入力できます。ホスト名は指定してもしなくても構いません(例: `index.html` あるいは `http://www.example.com/index.html`)。

間隔:チェック間隔を秒単位で入力します。デフォルトは 15秒です。つまり 15秒ごとに、すべての本サーバの健全性状態がチェックされます。

タイムアウト:本サーバが応答を送信する最大時間を秒単位で入力します。本サーバがこの時間内に応答しない場合、デッド(dead)とみなされます。

自動ファイアウォールルール(任意):このチェックボックスは、ゲートウェイルールを自動生成する場合に選択します。これらのルールにより、トラフィックをホストから実際のサーバに送ることができます。

仮想サーバアドレスのシャットダウン(任意):このチェックボックスは、追加のアドレスを負荷分散用の仮想サーバとして使用する場合(「*インターフェース > 追加アドレス*」の章を参照)のみに使用できます。すべてのリアルサーバが利用不可になった場合、追加アドレスインタフェースは自動的にシャットダウンされます。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
新しいルールが「*負荷分散*」リストに表示されます。

4. **負荷分散ルールを有効にします。**
新しいルールはデフォルトで無効になっています(トグルスイッチはグレー表示)。ルールを有効にするには、トグルスイッチをクリックします。

これでルールが有効になります(トグルスイッチは緑色)。

ルールを編集または削除するには、対応するボタンをクリックします。

例:IP アドレスが、それぞれ 192.168.66.10、192.168.66.20 の 2台の HTTP サーバが DMZ にある場合を想定します。ゲートウェイの外部インタフェースで受信した HTTP トラフィックを両方のサーバに均等に分散したいと仮定します。負荷分散ルールをセットアップするには、各サーバのホスト定義を選択あるいは作成します。それらを *http_server_1* および *http_server_2* とします。次に、「*新規負荷分散ルールの作成*」ダイアログボックスで、「*サービス*」として「*HTTP*」を選択します。さらに、「*仮想サーバ*」としてゲートウェイの外部アドレスを選択します。最後に、「*リアルサーバ*」ボックスにホスト定義を入力します。

重み分散およびインタフェースパーシスタンス

負荷分散サーバ間で重みを分散し、それらの間にインタフェースパーシスタンス設定するには、以下の手順に従ってください。

1. **負荷分散ルールの「*編集*」ボタンをクリックします。**
   「*負荷分散ルールの編集*」ダイアログボックスが開きます。

2. **「*バックエンドサーバ*」ボックスのヘッダで「*スケジューラ*」ボタンをクリックします。**
   「*スケジューラを編集*」ダイアログボックスが開きます。

3. **次の設定を行います。**
   加重:加重とは、あるサーバが処理するトラフィック量を他のサーバに対して相対的に示すもので、0～100 の間で設定できます。加重ラウンドロビンアルゴリズムが使用され、値が大きいほど、該当サーバにルーティングされるトラフィックが多くなります。相対的な値であるため、合計して 100にする必要はありません。たとえば、サーバ 1 の値を 100 に、サーバ 2 の値を 50 に、サーバ 3 の値を 0 に設定することなどができます。この場合、サーバ 2 のトラフィック量はサーバ 1 の半分となり、サーバ 3 は他のサーバが使用可能でない場合にのみ使用されます。0 の値は、より値が大きい他のサーバが常に使用されることを示します(他のインタフェースが使用可能であれば)。

   パーシスタンス:インタフェースパーシスタンスとは、クライアントからの後続の接続が常に同じアップリンクインタフェース経由でルーティングされるようにする技術です。パーシスタンスのデフォルトのタイムアウト時間は 1時間です。この負荷分散ルールのインタフェースパーシスタンスを無効化することもできます。

4. **「*保存*」をクリックします。**
   「*スケジューラの編集*」ダイアログボックスが終了し、設定が保存されます。

5. **「*保存*」をクリックします。**
   「*負荷分散ルールの編集*」ダイアログボックスが閉じます。

8.5 VoIP

VoIP (*Voice over Internet Protocol*) は、インターネットまたは他の IP ベースのネットワークを通した音声会話のルーティングです。Sophos UTMは、IP ネットワーク上で音声信号を伝送するために最もよく使用される次のプロトコルのサポートを提供しています。

- SIP
- H.323

8.5.1 SIP

Session Initiation Protocol(SIP)は 2つ以上の通信パートナー間のセッションの設定、変更、および終了のための信号を送るプロトコルです。SIP は主に音声またはビデオ通話の確立と終了処理に使用します。SIP を使用するには、まず、使用している IP アドレスと URL を、ISP で登録する必要があります。SIP は、ポート 5060 で UDP や TCP を使用して、メディアデータ(ビデオ、音声) をエンドポイント間で交換する際に使用する IP アドレスとポート番号を示します。すべてのアドレスに対してすべてのポートを開くとセキュリティに重大な問題が生じるため、SIP トラフィックは、高度な方法でゲートウェイで処理されます。これは、特別なコネクショントラッキングヘルパによって実現します。このヘルパは制御チャネルをモニタリングし、どの動的ポートが現在使用されているかを判断して、制御チャネルがビジーであるときはこれらのポートのみをトラフィックが通過するようにします。これを行うために、SIP プロトコルを介した通信を可能にする適切なファイアウォールルールを作成するために、SIP サーバネットワークと SIP クライアントネットワーク定義の両方を指定する必要があります。

SIPプロトコルのサポートを有効にするには、以下の手順に従います。

1. **「*SIP*」タブで、SIP プロトコルのサポートを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*グローバル SIP 設定*」エリアが編集可能になります。

2. **次の設定を行います。**
   SIP サーバネットワーク:ここで、SIP クライアントの接続先として許可される SIP サーバ (ISP が提供)を選択します。セキュリティ上の理由から、「*任意*」は選択しないでください。

   SIP クライアントネットワーク:SIP 通信の開始や応答を許可される SIP クライアントのホスト/ネットワークを選択します。SIP クライアントとは LAN 内のエンドポイントであり、他の SIP クライアントとのリアルタイムな双方向通信に関与します。

待機モード:通信セッションのチェックレベルを指定します。

- **厳密:**ISP のレジストラ(「REGISTER SIP」メッセージの送信先 IP アドレス)からの着信通話のみ許可します。さらに、UTM は、通信したエンドポイント(SIP メッセージを交換したデバイス)からのメディア(音声、ビデオ)データセッションのみを許可します。SIP メッセージとは異なる IP アドレスからメディアデータを 送信するプロバイダがありますが、これは、UTM によって拒否されます。
- **クライアント/サーバネットワーク:**定義済みのすべての SIP サーバネットワークやクライアントネットワークからの着信通話を許可します。IP アドレスが、定義済みの SIP サーバネットワークやクライアントネットワークに所属する場合、SIP メッセージを送信した IP アドレスとは異なる IP アドレスからのメディアデータを許可します。
- **任意:**あらゆるアドレスからの着信通話およびメディアデータを許可します。

3. **「*適用*」をクリックします。**
   設定が保存されます。

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

8.5.2 H.323

H.323 とは、ITU-T *(国際電気通信連合)*が公開した国際マルチメディア通信プロトコル標準であり、あらゆるパケット交換網上で音声・映像通信セッションを提供するプロトコルを規定しています。H.323 は、VoIP *(ボイスオーバー IP)*や IP ベースのテレビ会議で一般的に使用されます。

H.323 では、ポート1720 で TCP を使用して、エンドポイント間で使用する動的ポート範囲をコールのセットアップ時にネゴシエートします。動的範囲内ですべてのポートを開くと、セキュリティ上で重大な問題が発生するため、ゲートウェイはインテリジェントベースで H.323 関連のトラフィックを許可することができます。これは、特別なコネクショントラッキングヘルパによって実現します。このヘルパは制御チャネルをモニタリングし、どの動的ポートが現在使用されているかを判断して、制御チャネルがビジーであるときはこれらのポートのみをトラフィックが通過するようにします。この目的を達成するためには、H.323 プロトコルでの通信を可能にする適切なファイアウォールルールを作成するために、H.323 ゲートキーパとクライアントネットワーク定義の両方を指定する必要があります。

H.323 プロトコルのサポートを有効にするには、以下の手順に従います。

1. **「*H.323*」タブで、H.323 プロトコルのサポートを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*グローバル H.323 設定*」エリアが編集可能になります。

2. **次の設定を行います。**
   H.323 ゲートキーパ:H.323 ゲートキーパを選択します。H.323 ゲートキーパは、ゾーン内のすべての H.323 クライアント（マイクロソフトの NetMeeting などのエンドポイント）をコントロールします。より具体的には、ゲートキーパは LAN 上のゾーン内のすべての H.323 コールに対するモニタとして機能します。ゲートキーパの最重要タスクは、シンボルエイリアスアドレスと IP アドレスとの変換です。

   H.323 クライアント:ここで、H.323 接続を開始する元のホスト/ネットワークと宛先のホスト/ネットワークを選択できます。H.323 クライアントとは LAN 内のエンドポイントであり、他の H.323 クライアントとのリアルタイムな双方向通信に関与します。

   厳密モードを有効化（任意）:セキュリティを強化するには、このオプションを選択します。ただし、ISP との接続で問題が発生する場合は、厳格モードを無効にしてください。

3. **「*適用*」をクリックします。**
   設定が保存されます。

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

8.6 詳細

「*ネットワークプロテクション > 詳細*」メニューのタブを使用すると、ジェネリックプロキシ、SOCKS プロキシ、IDENT リバースプロキシなど追加のネットワークプロテクション機能を設定することができます。

8.6.1 ジェネリックプロキシ

ジェネリックプロキシ（別名「ポートフォワーダ」）は、DNAT とマスカレーディングの両機能を組み合わせており、特定のサービスへのすべての受信トラフィックを任意のサーバに転送（フォワーディング）します。標準 DNAT との違いは、ジェネリックプロキシでは外部への接続時にもリクエストの送信元 IP アドレスをインタフェースの IP アドレスに書き換える点です。さらに、宛先（ターゲット）ポート番号も変更することができます。

ジェネリックプロキシルールを追加するには、次の手順に従います。

1. **「ジェネリックプロキシ」タブで、「*新規ジェネリックプロキシルール*」をクリックします。**
   「*新規ジェネリックプロキシルールの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   インタフェース:受信接続のインタフェースを選択します。

サービス:プロキシを使用するトラフィックのサービス定義を選択します。

ホスト:トラフィックの転送先とするターゲットホストを選択します。

サービス:プロキシを使用するトラフィックのターゲットサービスを選択します。

許可ネットワーク:ポート転送を適用するネットワークを選択します。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しいルールが「*ジェネリックプロキシ*」ルールリストに表示されます。
4. **ジェネリックプロキシルールを有効にします。**
   新しいルールはデフォルトで無効になっています(トグルスイッチはグレー表示)。ルールを有効にするには、トグルスイッチをクリックします。

   これでルールが有効になります(トグルスイッチは緑色)。

ルールを編集または削除するには、対応するボタンをクリックします。

8.6.2 SOCKS プロキシ

SOCKS とは、クライアントサーバ型アプリケーションがネットワークファイアウォールのサービスを透過的に使用できるようにするインターネットプロトコルです。ファイアウォール内にある多くのクライアントアプリケーションが、インターネット上のホストと通信するために使用します。例としては、IRC/インスタントメッセージングクライアント、FTP クライアントや、Windows SSH/Telnet クライアントです。ファイアウォールの内側にあるこれらのクライアントは、外側にあるサーバにアクセスしたい場合、その代わりに SOCKS プロキシサーバに接続します。このプロキシサーバは、クライアントが外部サーバにアクセスする適格性をコントロールし、要求をサーバに受け渡します。クライアントアプリケーションは、SOCKS 4 または SOCKS 5 というプロトコルバージョンを明示的にサポートしている必要があります。

SOCKS のデフォルトポートは `1080` です。ほぼすべてのクライアントにこのデフォルトポート設定が導入されているため、通常は設定不要です。SOCKS と NAT の違いは、SOCKS が「バインド」要求(クライアントの代わりにポートでリスンする機能。わずかなクライアントだけがこれをサポートしています)もサポートしており、SOCKS 5 ではユーザ認証が可能である点です。

SOCKS プロキシを有効にする場合、プロキシへのアクセス権がある 1つ以上のネットワークを定義しなければなりません。ユーザ認証が必要である場合、SOCKS プロキシの使用を許可するユーザまたはグループも選択する必要があります。

注 – ユーザ認証を使用しない場合、SOCKS プロキシは SOCKS 4 プロトコルと SOCKS 5 プロトコルの両方で使用できます。ユーザ認証を選択した場合、SOCKS 5 のみが機能します。プロキシに SOCKS 5 モードでホスト名を解決させる場合、DNS プロキシも有効にする必要があります。有効にしないと、DNS 解決は失敗します。

SOCKS プロキシを設定するには、次の手順に従ってください。

1. **「*SOCKS プロキシ*」タブで、SOCKS プロキシを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*SOCKS プロキシオプション*」エリアが編集可能になります。

2. **次の設定を行います。**
   許可ネットワーク:SOCKS プロキシの使用を許可するネットワークを選択します。

   ユーザ認証の有効化:このオプションを選択すると、ユーザは SOCKS プロキシへのログイン時にユーザ名とパスワードを入力しなければならなくなります。ユーザ認証をサポートしているのが SOCKS 5 のみであるため、SOCKS 4 は自動的に無効になります。

   許可ユーザ:SOCKS プロキシの使用を許可するユーザまたはグループを選択します。

3. **「*適用*」をクリックします。**
   設定が保存されます。

8.6.3 IDENTリバースプロキシ

IDENT プロトコルは、リモートサーバがアクセス元クライアントの身元を簡単に確認するために使用します。IDENT プロトコルは暗号化されず、スプーフィングが簡単ですが、多くのサービスではいまだにこのプロトコルを使用しており、場合によっては必須です。

IDENT リレーを設定するには、次の手順に従ってください。

1. **「*IDENT リバースプロキシ*」タブで、IDENT リレーを有効化します。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、「*グローバル設定*」エリアが編集可能になります。

2. **次の設定を行います。**
   内部ホストへの転送 (任意):IDENT クエリはゲートウェイの接続追跡の対象にならないため、マスカレーディングが使用されている場合は障害が発生します。ゲートウェイの内側にあるマスカレーディングされたホストに IDENT クエリを受け渡すためには、「*内部ホストへの*

転送」オプションを選択します。実際の IP 接続は転送されません。代わりに、ゲートウェイが内部クライアントに IDENT 応答を要求し、その文字列を要求元サーバに転送します。この方法は、主要 IRC クライアントと FTP クライアントに組み込まれた大部分の「ミニ IDENT」サーバで機能します。

デフォルト応答:IDENT リレーを有効にすると、ゲートウェイは IDENT 要求への応答をサポートします。システムは、接続を開始したローカルサービスを問わず常に、「*デフォルト応答*」ボックスに入力した文字列で応答します。

3. **「*適用*」をクリックします。**
   設定が保存されます。

9 Web プロテクション

この章では、Sophos UTMの基本的な Web プロテクション機能を設定する方法を説明します。

この章では、次のトピックについて説明します。

- Web フィルタリング
- Web フィルタリングプロファイル
- アプリケーションコントロール
- FTP プロキシ

Webadmin の「*Web プロテクション統計*」ページには、時間、トラフィック、ならびに上位ユーザのアクセス状況に基づいた最も使用頻度の高いアプリケーションおよびアプリケーションカテゴリ、また、最もアクセスの多いドメインの概要が表示されます。さらに、ブロックされた上位Web サイトカテゴリが表示されます。各セクションには「*詳細*」リンクがあります。リンクをクリックするとWebAdmin の該当するレポートセクションが表示され、詳細な統計情報を参照できます。

「*上位アプリケーション*」セクションでは、アプリケーション名の上にカーソルを合わせると、追加機能が 1つまたは 2つ表示されます。

- *Block* アイコンをクリックすると、現時点から該当アプリケーションがブロックされます。これにより、「*アプリケーション コントロール*」ページにルールが作成されます。このオプションは、Sophos UTMの正常なオペレーションに必要なアプリケーションに対しては利用できません。たとえば、WebAdmin トラフィックはブロックできません。これをブロックすると、ユーザ自身が WebAdmin からシャットアウトされてしまいます。未分類のトラフィックもブロックできません。
- *Shape* アイコンをクリックすると、当該アプリケーションのトラフィックシェーピングが有効になります。ダイアログウィンドウが開き、ルール設定を定義するよう要求されます。完了したら「*保存*」をクリックします。これにより、「*トラフィックセレクタ*」および「*帯域幅プール*」ページにルールが作成されます。
  シェーピングはインタフェース単位で機能するため、「*すべてのインタフェース*」フローモニタを閲覧している際はトラフィックシェーピングを利用できません。

注 – 収集される Web サーフィンデータはセッションベースです。近似値を得るために、上位ドメインおよびユーザのすべてのデータが以下のように収集されます。各 Web 要求は、トラフィック量および要求間隔を考慮に入れてログされます。5分間アクティビティがなく、ユーザあるいはドメインに対する要求が記録されないと、そのセッションは終了したものとみなされます。5分間アク

ティビティがない場合でもユーザがまだ Web ページを表示している可能性を考えて、「*経過時間*」の値には常に 1分余計に追加されます。レポーティングデータは 15分ごとに更新されます。クライアントが無効な URL を要求した場合、Web フィルタはその要求をログしますが、その要求に応えることはできません。これらのリンクは「*Web プロテクション統計*」ページでエラーとして計上されます。これらはレポーティングや Web フィルタのエラーではなく、ほとんどの場合、ページ作成者が Web コンテンツに無効または不正なリンクを配置したために発生します。

9.1 Web フィルタリング

「*Web プロテクション > Web フィルタリング*」メニューのタブを使用すると、Sophos UTMソフトウェアを HTTP/S キャッシングプロキシとして設定することができます。Sophos UTMの HTTP/S プロキシは、シンプルなキャッシングに加え、HTTP/S の使用が許可されているネットワークに対して豊富な Web フィルタ技術を提供しています。これには、シグニチャデータベースとスパイウェアフィルタリング技術が定期的に更新される2つの異なるウイルススキャンエンジンを使用したウイルスおよびスパイウェア感染の防御機能もあり、受信トラフィックと送信トラフィックの両方を保護します。さらにSophos UTMでは、高度な Web サイト分類を採用しており、世界最大のリアルタイム URL データベースを使用してさまざまな Web ページへのアクセスをコントロールできます。Sophos のエンドポイントソフトウェアと合わせて使用することで、Sophos UTM は外部ネットワークにあるエンドポイントマシンでも同じ Web ポリシーを適用し、監視することができます。*エンドポイント Web コントロール*を有効にするには、「*エンドポイントプロテクション > Web コントロール*」を参照してください。

9.1.1 グローバル

「*Web プロテクション > Web フィルタリング > グローバル*」タブでは、Web フィルタのグローバル設定を実行できます。

Web フィルタを設定するには、次の手順に従います。

1. **「グローバル」タブで、Web フィルタを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、「*グローバル Web フィルタリング設定*」エリアが編集可能になります。

2. **許可するネットワークを選択します。**

Web フィルタの使用を許可するネットワークを選択します。デフォルトで、Web フィルタはクライアント要求を TCP ポート 8080 でリスンし、「*許可ネットワーク*」ボックスにリストされたネットワーク内のすべてのクライアントに対して接続を許可します。

3. **HTTPS (SSL) トラフィックのスキャン:**
HTTP トラフィックに加え HTTPS トラフィックもスキャンする場合は、このチェックボックスにチェックを入れます。

4. **オペレーションのモードを選択します。**
ユーザ認証が必要なオペレーションモードを選択する場合には、Web フィルタの使用を許可するユーザとグループを選択する必要があります。次のオペレーションモードを使用できます。

   - **標準モード:**標準モードでは、Web フィルタはデフォルトでクライアント要求をポート 8080 で待機し、「*許可ネットワーク*」ボックスにリストされたネットワーク内のすべてのクライアントに対して接続を許可します。このモードで使用する場合、クライアントはブラウザの設定で Web フィルタに HTTP プロキシを指定していることが必要です。
   認証モードを選択します。

     - **なし:**認証を行わない場合に選択します。
     - **Active Directory SSO:**「*定義とユーザ > 認証サーバ > サーバ*」タブで、「*Active Directory シングルサインオン*」(SSO) を設定した場合、これを選択します。これにより、NTLM ユーザ認証が認証クライアントで使用されます。動作が保証されるのは Internet Explorer のみです。このモードで使用する場合、クライアントはブラウザの設定で Web フィルタに HTTP プロキシを指定していることが必要です。

       注 – Active Directory ユーザグループを定義する際、LDAP 文字列でなく、Active Directory グループやユーザ名を手動で入力することで、「*Active Directory グループ*」ボックスに必要なエントリを追加することを強く推奨します。例:LDAP 文字列、`CN=ads_group1,CN=Users,DC=example,DC=com` の代わりに `ads_group1` という名前を入力してください。

       注 – Kerberos を使用している場合、「*Active Directory グループ*」ボックスには、グループのみを追加してください。エントリがユーザの場合、Web フィルタによって許可されていません。

- **エージェント:**Sophos Authentication Agent (SAA)を使用する場合に選択します。Webフィルタを使用するためには、エージェントと認証を開始する必要があります。
- **Apple OpenDirectory SSO:**「*定義とユーザ > 認証サーバ > サーバ*」タブで「*LDAP*」を設定しており、Apple OpenDirectory を使用している場合、これを選択します。さらに、プロキシが正しく機能するようにするためには、「*Web プロテクション > Web フィルタリング > 詳細*」タブで、MAC OS X シングルサインオン Kerberos 鍵ファイルをアップロードする必要があります。このモードで使用する場合、クライアントはブラウザの設定で Web フィルタに HTTP プロキシを指定していることが必要です。Safari ブラウザは SSO をサポートしていません。
- **基本ユーザ認証:**このモードでは、各クライアントは、プロキシを使用する前にこのプロキシに対して自己認証する必要があります。サポートされる認証方式について詳しくは、「*定義とユーザ > 認証サーバ*」を参照してください。このモードで使用する場合、クライアントはブラウザの設定で Web フィルタに HTTP プロキシを指定していることが必要です。
- **eDirectory SSO:**「*定義とユーザ > 認証サーバ > サーバ*」タブで「*eDirectory*」を設定した場合、これを選択します。このモードで使用する場合、クライアントはブラウザの設定で Web フィルタに HTTP プロキシを指定していることが必要です。

  注 – eDirectory および Active Directory のシングルサインオン(SSO)モードの場合、Web フィルタはアクセス先の IP アドレスと資格情報を最大 15分間キャッシュします。Apple OpenDirectory SSO の場合、キャッシュできるのはグループ情報のみです。これは、認証サーバへの負荷を軽減するために行われます。逆に言うと、ユーザ、グループ、またはアクセスしているユーザのログインステータスの変更が Web フィルタによって反映されるまで、最大 15 分かかります。

許可ユーザ/グループ:ユーザ認証が必要な認証モードを選択する場合は、Web フィルタの使用を許可するユーザとグループを選択する必要があります。

- **透過モード:**透過モードでは、ポート 80 (SSL を使用している場合はポート 443)でクライアントブラウザアプリケーションが 行うすべての接続はインターセプトされ、クライアント側の設定なしでプロキシにリダイレクトされます。クライアントが Web フィルタサーバを意識することは全くありません。このモードの利点は、追加の管理やクライアント側での設定が不要であることで、短所は、処理できるのが HTTP (ポート80) 要求のみであることです。そのため、透過モードを選択すると、クライアントのプロキシ

設定は無効になります。

注 – 透過モードでは、Web フィルタは HTTP 要求から NTLM 認証ヘッダを削除します。さらに、Web フィルタはこのモードでは FTP 要求を処理できません。クライアントがこのようなサービスにアクセスする必要がある場合は、ファイアウォールでポート(21)を開く必要があります。一部の Web サーバは、ポート80 以外のポート経由でストリーミング動画や音声などのデータを送信します。これらの要求は、Web フィルタが透過モードで機能しているときは検知されません。このようなトラフィックにも対応したい場合には、他のモードを使用するか、これらを許可する明確なファイアウォールルールを入力する必要があります。

フル透過モード(オプション): クライアントの送信元 IP をゲートウェイの IP で置き換えず、そのまま維持する場合は、これを選択します。これは、クライアントがパブリック IP アドレスを使用しており、Web フィルタによって隠すべきではない場合に便利です。このオプションはブリッジモードのみで意味があるため、ブリッジモードでしか利用できません。

認証モードを選択します。

- **なし:**認証を行わない場合に選択します。
- **エージェント:**Sophos Authentication Agent(SAA)を使用する場合に選択します。Web フィルタを使用するためには、エージェントと認証を開始する必要があります。「*許可ユーザ/グループ*」テキストボックスで、Web フィルタの使用を許可するユーザやグループを選択または追加できます。
- **ブラウザ:**選択すると、Web フィルタへの自己認証のためのログインダイアログがユーザのブラウザに表示されます。このモードでは、クライアント側のブラウザ設定なしで、ユーザ名に基づく追跡、報告、およびサーフィンが可能になります。さらに、そのダイアログウィンドウに追加で免責条項を表示することができます。この場合、ユーザが先に進むためには、免責条項に同意する必要があります。免責条項について詳しくは、「*管理 > カスタマイズ > Web メッセージ*」の章を参照してください。

5. **「*適用*」をクリックします。**
   設定が保存されます。

重要 – SSL スキャニングを透過モードと組み合わせて有効にすると、一部の SSL 接続(SSL VPN トンネルなど)が失敗します。SSL VPN 接続を有効にするには、対応するターゲットホストを「*透過モードスキップリスト*」に追加します(「*Web プロテクション > Web フィルタリング > 詳細*」を参

照)。
さらに、自己署名証明書でホストにアクセスするには、「*証明書信頼性チェック*」オプションを選択して、これらのホストの除外を作成する必要があります。これにより、プロキシで証明書のチェックが行われません。

ライブログ

Web フィルタリングライブログは、Web 要求に関する情報を提供します。「*ライブログを開く*」ボタンをクリックすると、新しいウィンドウで Web フィルタリングライブログが開きます。

9.1.2 ウイルス/マルウェア対策

「*Web プロテクション > Web フィルタリング > ウイルス/マルウェア対策*」タブでは、ウイルス、ワーム、その他のマルウェアといった有害で危険なコンテンツを伝送する Web トラフィックからネットワークを保護することを目的とするオプションを設定することができます。

アンチウイルススキャン

送信および受信 Web トラフィックをスキャンするためには、「*アンチウイルススキャンを使用*」オプションを選択します。Sophos UTMは、最高のセキュリティを実現するさまざまなアンチウイルスエンジンを備えています。

- **シングルスキャン:**デフォルト設定。「*スキャン設定*」タブに定義されたエンジンを使用して最高レベルのパフォーマンスを実現します。
- **デュアルスキャン:**各トラフィックに対し、異なるウイルススキャナを使用してスキャンを 2回行うことにより、検出率を最大限に高めます。ベーシックガードサブスクリプションではデュアルスキャンは利用できません。

最大スキャンサイズ:アンチウイルスエンジンでスキャンする最大ファイルサイズを指定します。このサイズを超えるファイルはスキャン対象外となります。

注 – 最大サイズを超えるファイルのダウンロードを禁止する場合は、「*詳細*」ページの「*許可するダウンロードの最大サイズ*」の値を必要に応じて設定してください。

設定を保存するには「*適用*」をクリックします。

ファイル拡張子フィルタ

この機能では、ファイルの拡張子 (実行可能バイナリなど) に基づいて、「*ブロックするファイル拡張子*」ボックスにファイル拡張子がリストされている特定のタイプのファイルを Web トラフィックから

フィルタします。ファイル拡張子を追加したり、ブロック対象から外すファイル拡張子を削除したりすることができます。ファイル拡張子を追加するには、「*ブロックするファイル拡張子*」ボックスのプラスアイコンをクリックし、ブロックする拡張子（exe など）を入力します。区切り記号のドットは不要です。

設定を保存するには「*適用*」をクリックします。

注 – ZIP ファイルなど、アーカイブされたファイルを悪意あるコンテンツについてスキャンすることはできず、ウイルススキャナを通過します。アーカイブされたファイルに含まれるマルウェアからネットワークを保護するには、該当するファイル拡張子をブロックすることを考慮してください。

MIME タイプフィルタ

ブロックする MIME タイプを追加するには、「*ブロックする MIME タイプ*」ボックスの「+」アイコンをクリックし、MIME タイプを入力します（image/gif など）。ここではワイルドカード（*）を使用できます（audio/* など）。

アクティブコンテンツ除去

「*アクティブコンテンツ削除*」エリアでは、Web ページに埋め込まれたオブジェクト（例: マルチメディアファイル）など特定の Web コンテンツが自動的に削除されるように設定することができます。次の設定が可能です。

- **埋め込みオブジェクトの削除:**選択すると、この機能はすべての <OBJECT> タグを HTML ページから削除し、ActiveX、Flash、Java などの動的コンテンツを受信 HTTP トラフィックから除去します。
- **Javascript の無効化:**選択すると、この機能は HTML ページ内のすべての <SCRIPT> タグを無効にするため、HTML ページに埋め込まれた機能やインクルードされた機能が無効になります。

9.1.3 URL フィルタリング

「*Web プロテクション > Web フィルタリング > URL フィルタリング*」タブでは、特定の種類の Web サイトに対するアクセスをコントロールするデフォルト設定を構成できます。

注 – 常に、ホワイトリストに対する照会が先に行われます。つまり、各 Web サイトリクエストをホワイトリストと比較して、一致が見つからなかった場合、ブラックリストと比較します。ブラックリストとの一致が見つかると、Web サイトはブロックされます。

次の設定が可能です。

URL フィルタ

選択の *許可/ブロック*:選択した Web サイトカテゴリを許可するかブロックするかを決定します。次のオプションを使用できます。

- **以下でチェックしたカテゴリをブロック:**このオプションを選択すると、選択した Web カテゴリはブロックされますが、他のすべての Web カテゴリは許可されます。
- **以下でチェックしたカテゴリを許可:**このオプションを選択すると、選択した Web カテゴリを除くすべての Web カテゴリがブロックされます。

デフォルトオプションは「*許可*」です。「*ブロック*」に切り替えると、これに従って下のオプションの意味は「逆に」なり、表示されるテキストで「*ブロック*」が「*許可*」に(あるいはその逆に)置き換えられます。

注 – 分類データベースにアクセスするためには、アップストリームのファイアウォールで TCP ポート6000 または TCP ポート80 を開放する必要があります。親プロキシを設定している場合、データベースへのすべての要求は親プロキシ経由で送信されます。

スパイウェアの伝染及び通信をブロック:スパイウェアとは、ユーザに認識させることなくシステムを精査して、ユーザの行動を広告主に報告する悪意のあるソフトウェアです。このオプションを選択すると、サーバからクライアントへのトラフィックでスパイウェアを検出し、ブロックします。これにより、ネットワーク内のコンピュータが新しいスパイウェアに感染するのを防ぐことができます。さらに、この機能を有効にすると、すでにインストールされているスパイウェアアプリケーションについても検出し、トラフィックをブロックできます。この結果、スパイウェアが収集したユーザ情報がインターネットに送信されなくなります。このオプションは、ページの最初のオプションを「*許可*」に設定した場合に限り使用できます。

注 – スパイウェアカテゴリは、使用可能な 18グループのいずれにも割り当てることができません。したがって、「*スパイウェアの伝染及び通信をブロック*」チェックボックスにチェックを入れることによってのみ、スパイウェア提供者から防御することができます。

レピュテーションに基づき URL をブロック: Web サイトは「*信頼される*」、「*中立*」、「*疑わしい*」または「悪意のある」に分類できますが、「悪意のある」はリストされていません(これは、「悪意のある」がリストに含まれていると、該当するすべてのサイトに対してしきい値オプションをまったく使用しないことが許可されてしまうためです)。未分類の Web サイトを「*未確認 (Unverified)*」と呼びます。ネットワークからアクセスできる Web サイトがどのような評判を持つべきかを決定することができます。選択したしきい値を下回る Web サイトはブロックされます。このオプションは、ページの最初のオプ

ションを「*許可*」に設定した場合に限り使用できます。Web サイトの評判について詳しくは、http://www.trustedsource.org を参照してください。

ブロックする Web サイトカテゴリ:ブロックする Web サイトカテゴリを選択します。ここで選択する Web サイトカテゴリとその下位のサブカテゴリのマッピングは、「*Web プロテクション > Web フィルタリング > URL フィルタリングカテゴリ*」タブで変更できます。ページの最初のオプションを「*ブロック*」に設定した場合、このオプションは「*許可する Web サイトカテゴリ*」に変わります。

注 – Web サイトが正しく分類されていないと思われる場合は、次の URL レポートフォームを使用して新しいカテゴリをご提案いただけます。

カテゴリー未分類サイトへのアクセスをブロック:このオプションを選択すると、未知のコンテンツのある Web サイトをブラウザで開くことができなくなります。この機能は、好ましくないと思われる Web サイトが相応の分類をされていない場合のフォールバックセキュリティメカニズムと考えることができます。
この機能のメリットの 1つに、いわゆるフィッシング攻撃からユーザを保護できることがあげられます。一般にフィッシングメールには、偽造 Web サイトへの疑わしいリンクが記載されています。この目的は、ユーザをだまして個人情報や機密情報を提供させることです。まだ有害と分類されていない場合、これらのリンクは「*未分類 (Uncategorized)*」または「*疑わしい (Suspicious)*」カテゴリとなります。このオプションを選択すると、これらのカテゴリはブロックされます。これにより、フィッシングメッセージが送信されても、ユーザは偽造 URL を開くことができません。
ページの最初のオプションを「*ブロック*」に設定した場合、このオプションは「*未分類 Web サイトへのアクセスを許可*」に変わります。

ブロックする URL/サイト:特定の URL や Web サイト、または特定のドメインにある複数の Web ページを、そのカテゴリに関わらずブロックするには、ここに入力します。その結果、ここで定義した Web サイトが、許可するカテゴリに属している場合でも、ブロックすることができます。

1. **「+」(プラス)アイコンをクリックして、「*正規表現オブジェクトを追加*」ダイアログウィンドウを開きます。**
2. **次の設定を行います。**
   - **名前:**正規表現を説明する名前を入力してください。
   - **ドメイン:**すべて、または特定の Web ページをブロックするドメインを入力します。ドメイン名全体を入力する必要があることに注意してください。たとえば、www も含める必要があります。以下で指定する正規表現のいずれか 1つがこの URL に一致した場合、指定したドメインの Web ページはブロックされます。正規表現を指定しなかった場合は、ドメイン全体がブロックされます。

- **正規表現:**上で指定したドメインの特定の Web ページをブロックするには、正規表現を入力します。上でドメインを指定しなかった場合は、この正規表現がすべてのドメインに適用されます。正規表現によっては、対象の URL だけではなく、検索結果や類似 URL の一部にも一致してしまうため、意図しないブロックにつながる可能性があります。

  参照 – Web フィルタリングで正規表現を使用する方法の詳細は、Sophos サポートデータベースを参照してください。

  注 – Web ページはできるだけ詳細に指定してください。ドメインを指定せずに正規表現のみを指定すると、意図しないブロックにつながる可能性があります。

- **コメント**(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
4. **「*適用*」をクリックします。**

ページの最初のオプションを「*ブロック*」に設定した場合、このオプションは「*許可する追加 URL/サイト*」に変わります。

常に許可する URL/サイト:特定の URL や Webサイト、または特定のドメインにある複数の Web ページを、そのカテゴリやブロックリストに存在するかどうかに関わらず明示的に許可するには、ここに入力します。

「+」(プラス)アイコンをクリックして、「*正規表現オブジェクトを追加*」ダイアログウィンドウを開きます。上記のオプションの説明に従って、適切なデータを入力します。説明は、このオプションにも共通しています。

ページの最初のオプションを「*ブロック*」に設定した場合、このオプションは「*常にブロックする URL/サイト*」に変わります。

セーフサーチ

セーフサーチ: Google、Bing、Yahoo の各検索エンジンに対して SafeSearch の使用を強制することができます。セーフサーチフィルタは、子供にふさわしくないコンテンツ(犯罪や不正)を検索結果から削除します。有効にすると、Web フィルタ経由で Web サーフィンをするユーザはフィルタをオフにできません。

YouTube for Schools:これを有効にすると、ユーザが再生できる YouTube 動画は、YouTube EDU サブセクションの YouTube 動画かユーザの学校のアカウントでアップロードされている YouTube 動画に

制限されます。これが機能するためには、YouTube for Schools プログラムに登録して、スクール ID を取得し、それを以下に入力する必要があります。

注 – Sophos UTMでは、トップレベルドメインの `youtube.com` と `ytimg.com` に加え、一般的な動画がブロックされないことを確認する必要があります。

- **YouTube School ID:**「*YouTube for Schools*」を有効にした場合、スクール ID または YouTube から提供されたコードを入力する必要があります。

ブロックのバイパス

ブロックのバイパスを許可するユーザ/グループ:特定のユーザまたはグループに対し、デフォルトでブロックされるページへのアクセスを許可する場合には、これらのユーザ/グループをこのドラッグアンドドロップボックスに追加します。これにより、ブロックされるページに「*URL をブロック解除*」ボタンが表示されるようになります。このボタンをクリックすると新しいページが開き、ユーザは資格情報およびブロックページへのアクセスを希望する理由を入力できます。このユーザが、直接またはグループ経由でバイパスブロックボックスに含まれていれば、ブロックページにアクセスできるようになります。バイパスはログに記録され、レポートの一部となります(「*ログとレポート > Web プロテクション > Web 使用状況レポート*」を参照)。「*詳細*」タブの「*その他の設定*」セクションで定義した認証タイムアウトは、バイパスにも適用されます。

9.1.4 URL フィルタリングカテゴリ

「*Web プロテクション > Web フィルタリング > URL フィルタリングカテゴリ*」タブでは、Web サイトカテゴリのカテゴリグループへのマッピングをカスタマイズできます。これは「*URL フィルタリング*」タブで選択できます。Sophos UTMは、60種類の Web サイトカテゴリを識別し、アクセスをブロックすることができます。高度な URL 分類方法により、疑わしい Web サイトの識別における精度と完全性が保証されます。データベースに含まれていない Web ページをユーザが要求すると、URL が Web クローラに送信され、自動的に分類されます。

注 – Web サイトが正しく分類されていないと思われる場合は、次の URL レポートフォームを使用して新しいカテゴリをご提案いただけます。

Web サイトカテゴリをカテゴリグループに割り当てるには、次の手順に従ってください。

1. **編集するカテゴリグループで「編集」をクリックします。**
   「*フィルタカテゴリの編集*」ダイアログボックスが開きます。

2. **サブカテゴリを選択します。**
   グループに追加(またはグループから削除)するサブカテゴリのチェックボックスにチェックを入れます(またはチェックを外します)。

3. **「*保存*」をクリックします。**
   指定した設定でグループが更新されます。

あるいは、新しいフィルタカテゴリを作成することもできます。次の手順で実行します。

1. **ページ上部にある「*新規フィルタカテゴリ*」ボタンをクリックします。**
   「*フィルタカテゴリの作成*」ダイアログボックスが開きます。

2. **名前を入力します。**
   新しいフィルタカテゴリを説明する名前を入力してください。

3. **サブカテゴリを選択します。**
   グループに追加するサブカテゴリのチェックボックスを選択します。

4. **「*保存*」をクリックします。**
   指定した設定でグループが更新されます。

カテゴリを編集または削除するには、対応するボタンをクリックします。

9.1.5 除外

「*Web プロテクション > Web フィルタリング > 除外*」タブでは、クライアントネットワーク、ユーザ/グループ、ドメインのホワイトリストを定義できます。これらのリストに含まれるすべてのエントリを、特定の Web プロテクションサービスの対象外にすることができます。

除外ルールを作成するには、次の手順に従います。

1. **「*除外*」タブで、「*新規除外リスト*」をクリックします。**
   「*除外リストを作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:この除外ルールを説明する名前を入力してください。

   コメント(任意):説明などの情報を追加します。

   スキップするチェック:スキップするセキュリティチェックを選択します。

   - **認証:**Web フィルタを*認証*モードで実行している場合、送信元ホスト/ネットワークまたはターゲットドメインの認証をスキップできます。

- **キャッシング:**選択すると、特定のドメインまたは送信元ホスト/ネットワークのキャッシングが無効になります。
- **ダウンロードサイズでブロック**:選択すると、コンテンツのサイズに応じてダウンロードをブロックできます。
- **ウイルス対策:**選択すると、ウイルスやトロイの木馬などの好ましくないコンテンツがメッセージに含まれていないかチェックするウイルススキャンが無効になります。
- **拡張子ブロック:**選択すると、ファイル拡張子フィルタが無効になります。このフィルタは、拡張子に基づいて特定タイプのファイルが含まれるコンテンツをブロックするために使用します。
- **MIME タイプブロック:**選択すると、MIME タイプフィルタが無効になります。このフィルタは、特定の MIME タイプのコンテンツをブロックするために使用します。
- **URL フィルタ:**選択すると、URL フィルタが無効になります。このフィルタは、特定の種類の Web サイトへのアクセスをコントロールします。
- **コンテンツ削除:**選択すると、(マルチメディアファイルなどの)埋め込みオブジェクトや JavaScript といった Web ページ内の特殊コンテンツの削除がスキップされます。
- **SSL スキャン:**選択すると、要求された Web ページに対する SSL スキャンがスキップされます。これは、オンラインバンキングの Web サイトや、SSL インターセプションがうまく機能しない Web サイトなどで有用です。技術的な理由から、このオプションは透過 Web フィルタモードでは機能しません。透過モードでは、代わりに「*透過スキップリスト*」を使用してください(*詳細*」セクションを参照)。標準モードでは、クライアントが何を送信するのかに応じて、宛先ホストまたは IP アドレスのみに基づいて除外を行うことができます。URL 全体ではなくカテゴリに基づく除外では、ホスト名のみが分類されます。
- **証明書信頼性チェック:**選択すると、HTTPS サーバ証明書の信頼性チェックがスキップされます。Web フィルタが認証ありの透過モードで機能している場合、ユーザ/グループの照合に基づく証明書の信頼性チェックをスキップすることは技術的に不可能です(「*ユーザ/グループからの全リクエストに適用*」)。
- **証明書日付チェック:**選択すると、HTTPS 証明書の日付が有効であるかどうかのチェックがスキップされます。

労働協議会の会員など、活動内容を記録することが禁止されているユーザがいる場合には、次の 2つのオプションが便利です。

- **アクセスしたページ:**選択すると、アクセスしたページが記録されなくなります。これらのページ要求は、レポートからも除外されます。

- **ブロックしたページ:**選択すると、ブロックされたページが記録されなくなります。これらのページ要求は、レポートからも除外されます。

対象:セキュリティチェックをスキップする条件を少なくとも 1つ選択します。条件の前にあるドロップダウンリストで「*And*」または「*Or*」を選択して、複数の条件を論理的に組み合わせることができます。次の条件を設定できます。

- **送信元ネットワーク:**選択して、この例外ルールのセキュリティチェックから除外する送信元ホスト/ネットワークを追加します。条件を選択すると、「*ホスト/ネットワーク*」ボックスが開くので、各ホストまたはネットワークを入力します。
- **宛先 URL:**選択して、この除外ルールのセキュリティチェックから除外する対象ドメインを追加します。条件を選択すると「*ターゲットドメイン*」ボックスが開くので、各ドメインを追加します。ここでは、正規表現を使用することができます。例:`^https?://[^.]*\.domain.com` は、ドメインのすべてのサブドメインへのHTTP (S) 接続と一致します。

  参照 – Web フィルタリングで正規表現を使用する方法の詳細は、Sophos サポートデータベースを参照してください。

  注 – SSLスキャニングを有効にして*透過*モードを使用している場合、ターゲットドメインをIPアドレスで入力する必要があります。IP アドレスを入力しないと、除外は技術的な理由で失敗します。

- **送信元ユーザ/グループ:**選択して、この例外ルールのセキュリティチェックから除外するユーザやユーザグループを追加します。条件を選択すると「*ユーザ/グループ*」ボックスが開くので、各ユーザまたはグループを入力します。また、標準モードでは認証が存在しないため、特定のユーザ/グループの照合は機能しません。
- **宛先 Web サイトカテゴリ:**選択すると、特定のカテゴリに対するセキュリティチェックがスキップされます。条件を選択するとリストが開くので、カテゴリを選択します。

3. **「*保存*」をクリックします。**
   新しい除外が「*除外*」リストに表示されます。

除外ルールを編集または削除するには、対応するボタンをクリックします。

9.1.6 詳細

「*Web プロテクション > Web フィルタリング > 詳細*」タブには、キャッシングやポートの設定など、Web フィルタの各種設定オプションが用意されています。

その他の設定

Webフィルタリングポート:ここで、Web フィルタがクライアントのリクエストに対して使用するポート番号を定義できます。デフォルトは 8080 です。

注 – これが適用されるのは、プロキシを透過モードで操作していない場合のみです。

アクセスしたページのログ:選択すると、リクエストのユーザ名とクライアント IP とともに、アクセスした URL のログが記録されます。

ブロックしたページのログ:選択すると、リクエストのユーザ名とクライアント IP とともに、ブロックした URL のログが記録されます。

注 – ログオプションは、除外(「*Web フィルタリング* > *除外*」の章を参照)またはプロファイルのフィルタアクション(「*Web フィルタリングプロファイル* > *フィルタアクション*」の章を参照)を利用して個別に設定することもできます。

スキャンできないファイル、暗号化されたファイルのブロック:このオプションを選択して、スキャンできなかったファイルをブロックします。スキャンできない理由はいくつかありますが、ファイルが暗号化されているか、破損している可能性があります。

MIME ブロックによる HTTP ボディの検査:HTTP ヘッダのみならず、HTTP ボディも、ブロック対象 MIME タイプに対してチェックされます。この機能をオンにすると、パフォーマンスが低下する可能性があります。

許可するダウンロードの最大サイズ:指定したサイズ(MB)を超えるファイルのダウンロードを禁止する場合にこのオプションを選択します。

注 – 「*ストリーミング設定*」セクションで「*ストリーミングコンテンツに対するスキャンをバイパス*」チェックボックスが選択されていない場合、ユーザのストリーミングコンテンツはここで指定したサイズで制限されます。

許可するターゲットサービス:「*許可されるターゲットサービス*」ボックスでは、Web フィルタのアクセスが許可されるターゲットサービスを選択できます。デフォルト設定は、*HTTP*(ポート 80)、*HTTPS*(ポート 443)、*FTP*(ポート 21)、*LDAP*(ポート 389)、*LDAP-SSL*(ポート 636)、*Web フィルタ*(ポート 8080)、*Spam Release*(ポート 3840～ 4840)、および *UTMWebAdmin*(ポート 4444)などのターゲットサービス(ポート)で構成されています。これらは、通常は安全に接続でき、ブラウザで一般に使用されています。

デフォルトの文字コード:このオプションは、「*ダウンロードマネージャ*」ウィンドウでプロキシがファイル名をどのように表示するかに影響を与えます。外国語の文字セットでエンコードされている URL (および URL で参照されるファイル名) は、サーバが別の文字セットを送信する場合を除き、ここで指定されている文字セットから UTF-8 に変換されます。ダブルバイト文字セットを使用する国または地域では、このオプションを当該国または地域の「ネイティブ」文字セットに設定する必要があります。

検索ドメイン:ここで、最初の DNS ルックアップで結果が返されなかった (″NXDOMAIN″) 場合に検索される追加のドメインを追加することができます。最初の DNS ルックアップの次に、2番目の DNS 要求が開始され、ここで指定したドメインをオリジナルのホスト名に追加します。例:ユーザがアドレス *wiki.intranet.example.com* として「`http://wiki`」と入力します。ただし、URL は、「*ドメイン検索*」フィールドに「`intranet.example.com`」と入力していなければ解決できません。

認証タイムアウト:このオプションを使用すると、透過的なユーザ認証機能またはブロックの回避機能を使用しているときにユーザに認証を求める間隔を秒単位で設定できます。

認証レルム:認証レルムとは、プロキシが *基本ユーザ認証* モードで機能しているときに、ブラウザが認証要求とともに表示する送信元の名前です。認証レルムは、RFC 2617 に基づいて保護スペースを定義します。ここでは任意の文字列を指定できます。

透過モードスキップリスト

このオプションは、Web フィルタを透過モードで実行している場合のみ有用です。「*透過モード時にスキップするホスト/ネット*」ボックスにリストされたホストとネットワークは、HTTP トラフィックの透過的なインターセプションの対象外となります。ボックスは、送信元ホスト/ネットワーク用に 1つ、宛先ホスト/ネットワーク用に 1つあります。これらのホストとネットワークに対して、HTTP トラフィックを (プロキシなしで) 許可するには、「*リスト内のホスト/ネットワークの HTTP/S トラフィックを許可*」チェックボックスにチェックを入れます。このチェックボックスにチェックを入れない場合は、ここでリストされているホストとネットワークに特定のファイアウォールルールを定義する必要があります。

Proxy Auto Configuration (プロキシの自動設定)

プロキシの自動設定とは、ブラウザにフェッチされるプロキシ自動設定ファイル (PAC ファイル) を一元的に提供するための機能です。ブラウザはこれを受けて、PAC ファイルに記述された詳細に従ってプロキシ設定を構成します。

PAC ファイルの名前は *wpad.dat*、MIME タイプは `application/x-ns-proxy-autoconfig` で、UTM から提供されるものです。このファイルには、たとえば次のように、テキストボックスに入力した情報が含まれています。

```
function FindProxyForURL(url, host)
 { return "PROXY proxy.example.com:8080; DIRECT"; }
```

上の関数は、すべてのページ要求をポート8080上の proxy.example.comというサーバのプロキシにリダイレクトするようブラウザに指示しています。プロキシに到達できなければ、インターネットへの直接接続が確立されます。

ホスト名は、${asg_hostname}という変数としても指定できます。これは、Sophos UTM Managerを使用して、同じPACファイルを複数のSophos UTMアプライアンスにインストールする場合などに便利です。変数には、該当するUTMのホスト名が挿入されます。上記の例にある変数を使用すると、次のようになります。

```
function FindProxyForURL(url, host)
 { return "PROXY ${asg_hostname}:8080; DIRECT"; }
```

ネットワークでPACファイルを提供するには、次の方法があります。

- ブラウザ設定経由で提供する:「*プロキシ自動設定の有効化*」オプションを選択すると、UTM Webフィルタ経由でPACファイルを使用できるようになります。このとき、次のようなURLを使用します。http://IP-of-UTM:8080/wpad.datこのファイルを使用するには、プロキシを使用するブラウザの自動プロキシ構成設定にこのURLを入力します。
- DHCP経由で提供する:DHCPサーバがクライアントのIPアドレスと併せてPACファイルのURLを受け渡すようにすることもできます。これには、DHCPサーバの設定で「*HTTP プロキシ自動設定の有効化*」オプションを選択します(「*ネットワークサービス > DHCP*」の章を参照してください)。これにより、ブラウザがPACファイルを自動的に取得し、それに従って設定を構成します。

  注 – DHCP経由での提供は、マイクロソフトのInternet Exploreのみで機能します。その他すべてのブラウザでは、PACファイルを手動で提供する必要があります。

HTTP/S 親プロキシルーティング

親プロキシは、多くの場合、政府承認のプロキシサーバを通してインターネットアクセスをルーティングする必要のある国などで必要とされます。1つ以上の親プロキシの使用がセキュリティポリシーで求められている場合、ここで親プロキシを追加または選択できます。

ボックスが空の場合、まず、親プロキシの定義を作成してください。以下の手順に従ってください。

1. **ボックスヘッダの「+」アイコンをクリックします。**
   「*親プロキシの追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:この親プロキシを説明する名前を入力してください。

   コメント(任意):説明などの情報を追加します。

プロキシを使用するホスト:親プロキシを使用するホストをこのボックスに追加します(例: `*.wikipedia.org`)。ここではパターンマッチを使用できます。ただし、正規表現は使用できません。ボックスを空にすると、「*保存*」をクリックするとアスタリスク(*)が自動的に追加され、すべてのホストに該当します。従って、このようなプロキシ定義は、一致するプロキシが存在しない場合のフォールバックプロキシとみなされます。

親プロキシ:親プロキシのネットワーク定義を選択または追加します。

ポート:親プロキシ接続のデフォルトポートは 8080 です。親プロキシで別のポートを使用する場合、ここで変更できます。

プロキシ認証が必要:親プロキシが認証を必要とする場合は、チェックボックスにチェックを入れ、表示されるテキストボックスにユーザ名とパスワードを入力します。

3. **「*保存*」をクリックします。**
   新しい親プロキシが「*親プロキシ*」ボックスに表示されます。

これで、このプロキシをフィルタアクションで使用することも、グローバルに使用することもできます。親プロキシ定義を編集または削除するには、「*Web フィルタリングプロファイル > 親プロキシ*」タブにアクセスします。

各プロキシの前にあるチェックボックスにチェックを入れて、親プロキシの使用を有効化します。複数のプロキシを選択した場合、「並び替え」アイコンを使用してプロキシを並べ替えることができます。選択した親プロキシは、最初のプロキシが一致するまで、所定の順序で適用されます。処理順序は位置番号によって決まるため、位置番号によってプロキシの順序を変更すると、処理順序も変わります。

親プロキシの使用は、プロファイルベースにすることもできます(詳しくは、「*Web フィルタプロファイル > フィルタアクション*」の章を参照してください)。

親プロキシおよび Web サイトカテゴリ

親プロキシ経由でデータベース更新の取得やカテゴリのルックアップを行いたい場合は、この親プロキシに対して以下のホストを指定する必要があります。

- `list.smartfilter.com`(ローカルカテゴリデータベースの場合)
- `cffs*.astaro.com`(TCP でのカテゴリ取得の場合)

1つの親プロキシがすべてのホストに一致するように設定する場合(*)、これらのホストを指定する必要はありません。特定のホストに対して異なる親プロキシを定義し、最後の親プロキシがすべてのホストに一致するように(*)設定することもできます。この場合、このトラフィックのみが最後の親プロキシ経由でルーティングされ、他のすべての親プロキシは一致しません。

Web キャッシング

キャッシングの有効化:このオプションが有効になっている場合、Web フィルタはオンディスクオブジェクトキャッシュを保持して、アクセス頻度が高い Web ページへの要求を高速化します。

- **SSL コンテンツのキャッシュ:**このオプションを有効にすると、SSL 暗号化されたデータは、暗号化されていない状態でディスクに保存されます。
- **cookie を含むコンテンツをキャッシュ:**Cookie は、一般に認証目的で使用されます。このオプションを有効にすると、Cookie が含まれる HTTP 応答もキャッシュされます。複数のユーザが同じページを要求している場合、あるユーザの Cookie が含まれるキャッシュページが他のユーザに提供される可能性があるため、この設定は重大です。

  重要 – SSL または Cookie コンテンツ(あるいはその両方)をキャッシュすると、SuperAdmin 権限を持つすべてのユーザがコンテンツを閲覧できるため、セキュリティ上の重要な問題です。

- **Sophos エンドポイント用アップデートの強制キャッシュ:**有効にすると、エンドポイントからの Sophos Auto Update(SAU)リクエストに関する特定のデータがキャッシュされます。エンドポイントプロテクションを使用する際は、この機能を有効にすることを推奨します。無効にすると、この種のデータはキャッシュされません。この場合、インターネット経由で、同時に多数のエンドポイントが、アップデートサーバからデータをダウンロードしようとするアップリンクの飽和が発生する恐れがあります。

キャッシュをクリア:「*キャッシュをクリア*」をクリックすると、キャッシュされたすべてのページを削除できます。

ストリーミング設定

ストリーミングコンテンツに対するコンテンツスキャンのバイパス:このオプションを選択すると、一般的な音声・動画ストリーミングコンテンツがコンテンツスキャンの対象外となります。このオプションを無効にすると、大部分のメディアストリームは事実上無効になります。これは、このようなストリームを合理的な時間内でスキャンすることができないためです。そのため、このオプションは選択することを推奨します。

Apple OpenDirectory シングルサインオン

認証方式として *Apple OpenDirectory SSO* を使用している場合、認証が適切に機能するためには、MAC OS X シングルサインオン Kerberos 鍵ファイルをアップロードする必要があります。鍵ファイルを生成し、フォルダアイコンをクリックしてアップロードします。鍵ファイルの生成方法について詳しくは、Kerberos のマニュアルを参照してください。

9.1.7 HTTPS CA

「*Web プロテクション > Web フィルタリング > HTTPS CA*」タブでは、HTTPS 接続の署名および検証 CA（認証局）を管理できます。

署名 CA

このエリアでは、署名 CA 証明書のアップロード、署名 CA 証明書の再生成、または既存の署名 CA 証明書のダウンロードが可能です。デフォルトで署名 CA 証明書は、セットアップ中に提供された情報に基づいて作成されます。つまり、セットアップ後に何らかの変更が行われた場合を除き、「*マネジメント > システム設定 > 組織*」タブの情報と整合性があります。

新しい署名 CA 証明書をアップロードするには、次の手順に従ってください。

1. **「アップロード」ボタンをクリックします。**
   「*PKCS#12 証明書ファイルのアップロード*」ダイアログウィンドウが開きます。
2. **アップロードする証明書までブラウズします。**
   「*ファイル*」ボックスの横にあるフォルダアイコンをクリックし、「*ファイルのアップロード*」ダイアログボックスが開いたら「*参照*」をクリックしてアップロードする証明書を選択し、「*アップロード開始*」をクリックします。

   パスワードで保護されている PKCS#12 形式の証明書のみをアップロードできます。
3. **パスワードを入力します。**
   該当フィールドにパスワードをもう一度入力し、「*保存*」をクリックします。

   新しい署名 CA 証明書がインストールされます。

署名 CA 証明書を再生成するには、次の手順に従ってください。

1. **「再生成」ボタンをクリックします。**
   「*新規署名 CA の作成*」ダイアログボックスが開きます。
2. **情報を変更します。**
   必要に応じて所定の情報を変更し、「*保存*」をクリックします。

   新しい署名 CA 証明書が生成されます。これに基づき、「*署名 CA*」エリア内の署名CA情報が変化します。

署名 CA 証明書をダウンロードするには、次の手順に従ってください。

1. **「ダウンロード」ボタンをクリックします。**
   「*証明書ファイルのダウンロード*」ダイアログボックスが開きます。

2. **ダウンロードするファイル形式を選択します。**
   2種類の形式から選択できます。
   - **PKCS#12:**この形式は暗号化されるため、エクスポートパスワードを入力してください。
   - **PEM:**暗号化されない形式です。
3. **「*ダウンロード*」をクリックします。**
   ファイルがダウンロードされます。

カスタム CA で署名された証明書を内部 Web サーバに対して使用する場合、信頼される認証局としてこの CA 証明書を WebAdmin にアップロードすることをお勧めします。これを行わないと、Web フィルタが、信頼できないサーバ証明書が検知されたというエラーメッセージをユーザに表示します。
クライアント PC へのプロキシ CA 証明書の提供を円滑化するために、ユーザは自分で http://passthrough.fw-notify.net/cacert.pem から証明書をダウンロードし、ブラウザにインストールすることができます。Web サイト要求はプロキシで直接受信され、処理されます。そのため、まず「*Web セキュリティ > グローバル*」タブで Web フィルタを有効にする必要があります。

注 – プロキシのオペレーションモードが*透過モード*ではない場合、ユーザのブラウザでプロキシを有効にする必要があります。有効にしないと、証明書ダウンロード用のリンクがアクセス不可になります。

あるいは、ユーザポータルが有効であれば、ユーザはプロキシ CA 証明書をユーザポータルの「*HTTPS プロキシ*」タブからダウンロードできます。

HTTPS での問題を回避する

HTTPS の使用中、Windows Update や Windows Defender などの Windows システムプログラムは接続を確立できません。これは、これらのプログラムがシステムユーザ権限で実行されるためです。このユーザはデフォルトで、プロキシ CA を信頼しないことになっています。そのため、システムユーザ用に HTTPS プロキシ CA 証明書をインポートする必要があります。以下の手順に従ってください。

1. **Windowsで、*Microsoft 管理コンソール* (mmc) を開きます。**
2. **「*ファイル*」メニューをクリックし、「*スナップインの追加と削除*」をクリックします。**
   「*スナップインの追加と削除*」ダイアログウィンドウが開きます。
3. **ウィンドウの一番下にある「*追加*」をクリックします。**
   「*スタンドアロン スナップインの追加*」ダイアログウィンドウが開きます。

4. **リストから「*証明書*」を選択し、「*追加*」をクリックします。**
   ウィザードが表示されます。
5. **「*コンピュータ アカウント*」を選択し、「*次へ*」をクリックします。**
6. **「*ローカル コンピュータ*」が選択されていることを確認し、「*完了*」>「*閉じる*」をクリックします。**
   最初のダイアログウィンドウに「*証明書*」が追加されています。
7. **「*OK*」をクリックします。**
   ダイアログウィンドウが閉じて、コンソールルートに「*証明書*」が追加されています。
8. **左側の「*コンソール ルート*」ウィンドウで「*証明書 > 信頼されたルート証明機関*」を開き、「*証明書*」を右クリックして、コンテキストメニューの「*すべてのタスク > インポート*」を選択します。**
   インポートダイアログウィザードが開きます。
9. **「*次へ*」をクリックします。**
   次のウィザードステップが表示されます。
10. **以前にダウンロードしたHTTPSプロキシCA証明書までブラウズし、「*開く*」>「*次へ*」をクリックします。**
    次のウィザードステップが表示されます。
11. **「*証明書をすべて次のストアに配置する*」が選択されていることを確認し、「*次へ*」>「*閉じる*」をクリックします。**
    インポートの成功がウィザードから報告されます。
12. **ウィザードのメッセージを確認します。**
    信頼される証明書の中に、プロキシCA証明書が表示されるようになりました。
13. **変更を保存します。**
    「*ファイル*」メニューをクリックし、「*保存*」をクリックして、コンソールルートでの変更を保存します。

インポート後、CA はシステム全体で受け入れられるようになり、HTTPS プロキシに起因する接続問題は発生しなくなります。

検証 CA

このエリアでは検証 CA を管理できます。検証 CA とは、最初に信頼する認証局です。つまり、これらの CA によって署名された有効な証明書を提示する Web サイトは、HTTPS プロキシによって信頼できると見なされます。

ローカル検証 CA:下の CA リストに追加して検証 CA をアップロードできます。次の手順で実行します。

1. **「*ローカル CA のアップロード*」フィールドの横のフォルダアイコンをクリックします。**
   「*ファイルのアップロード*」ダイアログボックスが開きます。
2. **アップロードする証明書を選択します。**
   「*参照*」をクリックして、アップロードする CA 証明書を選択します。次の証明書の拡張子がサポートされています。
   - `cer`、`crt`、または `der`:これらの証明書タイプはバイナリで、基本的には同じです。
   - `pem`:Base64 で暗号化された DER 証明書。
3. **証明書をアップロードします。**
   「*アップロード開始*」をクリックして、選択した CA 証明書をアップロードします。

   証明書はインストールされ、「*ローカル検証 CA*」エリアに表示されます。

グローバル検証 CA:ここに表示される検証 CA のリストは、Mozilla Firefox にあらかじめインストールされた検証 CA と同じです。ただし、リストに含まれるいずれか（あるいは全部）の検証 CA を「信頼できない」場合は、これらを無効にすることができます。CA の証明書を無効にするには、該当のトグルスイッチをクリックします。トグルスイッチが灰色になり、HTTPS プロキシはこの CA に署名された Web サイトを受け入れなくなります。

ヒント – CA のフィンガープリントを表示するには、青色の情報アイコンをクリックしてください。

CA が不明または無効である場合、HTTPS プロキシはクライアントに対して「ブロックされたコンテンツ」のエラーページを表示します。ただし、このようなページに対して除外を作成することができます。これには、Web フィルタのエラーページで「*除外の作成*」リンクを使用するか、「*Web プロテクション > Web フィルタリング > 除外*」タブを使用します。

注 – Webフィルタのエラーページで「*除外の作成*」リンクをクリックすると、ログインダイアログウィンドウが表示されます。admin 権限のあるユーザのみが除外を作成できます。

9.2 Web フィルタリングプロファイル

Sophos UTM には、どのネットワークに対して何の Web コンテンツを利用可能にするかをコントロールするために設計、最適化された Web フィルタが用意されています。これにより、好ましくないと考えるコンテンツを利用者が閲覧することを予防できます。Web フィルタを設定し、選択したネットワークに対してグローバルに適用することができます。あるいは、ネットワークのセグメント別に各種セキュリティポリシーを適用するために個々の Web フィルタプロファイルを作成することができま

す。これにより、ユーザ認証方式が異なる場合でも、組織内の各部門に適した別々のコンテンツフィルタリングポリシーを定義することができます。

この章では、Sophos UTMでのフィルタアクションの追加方法と、Web フィルタプロファイルフレームワークでフィルタアクションを使用する方法について説明します。「*Web フィルタリングプロファイル*」タブの設定は、後方から前方に向かって進めることをお勧めします。つまり、フィルタアクションの指定から開始します。これらは、フィルタ割り当てで特定のユーザまたはユーザグループに割り当てます。次に、実際の Web フィルタリングプロファイルの設定に続きます。

9.2.1 概要

注 – Web フィルタリングプロファイルを設定するためには、Web フィルタリングを有効にする必要があります。

このフローチャートは、フィルタアクション、フィルタ割り当て、Web フィルタプロファイルの間でどのようなやり取りがあるのかを示します。HTTP リクエストを受け取ると、Web フィルタはまず、どの Web フィルタプロファイルを適用すべきか判断します。これは、リクエストの送信元 IP アドレスに完全に依存します。リクエストの送信元 IP と一致する最初のプロファイルが使用されます。他のすべての Web フィルタプロファイルは無視されます。

内部では、すべてのプロファイルが1つのファイルに保存され、デフォルトプロファイルはリストの一番下に配置されます。他の HTTP プロファイルが設定されていない初期段階には、デフォルトプロファイルが唯一のエントリとなります。個々の Web フィルタプロファイルを追加して、「*位置*」ドロップダウンリストでプロファイルをソートするようになると、デフォルトプロファイルはリストの一番下に留まり、常に一番最後に適用されるようになります。

ただし、デフォルトプロファイルは、「*Web プロテクション > Web フィルタプリングロファイル*」タブで明示的に設定するプロファイルでは*ありません*。「*Web プロテクション > Web フィルタリング*」タブで Web フィルタをグローバルに設定すると自動的に作成されます。「*許可ネットワーク*」は、Web フィルタリングプロファイルの*送信元ネットワーク*に対応する「*Web プロテクション > Web フィルタリング > グローバル*」タブで設定します。「*ユーザ/グループ*」ボックスの設定（オペレーションモード「*基本ユーザ認証*」を選択すると「*Web プロテクション > Web フィルタリング > グローバル*」タブに表示される）は、デフォルトのフィルタ割り当てとなります。また、「*Web プロテクション > Web フィルタリング > URL フィルタリング*」タブの設定は、フィルタアクションに対応します。最後に、デフォルトプロファイルでも一致しなかった場合、HTTP 要求はブロックされます。

続いて、この Web フィルタプロファイルにどのフィルタ割り当てが関連付けられているのかをチェックします。フィルタ割り当てが一致しない場合、フォールバックアクションが要求に適用されます。フォールバックアクションとは、御社のセキュリティポリシーを反映させるための特別なフィル

タアクションです。厳格なセキュリティポリシーを遵守する必要がある場合、例外なくすべての Web トラフィックをブロックするフィルタアクションを作成することができます。

同じネットワークセグメント内の複数のユーザに対して、異なるレベルの防御を提供するには、異なるフィルタ割り当てを関連付けて 1つの Web フィルタプロファイルを設定するだけです。特定のユーザに何が許可されるのかは、選択したフィルタ割り当ての順番に応じて決まります。このため、送信元ネットワークがまったく同じである 2つのプロファイルを設定しても、2つ目のプロファイルはまったく使用されないため、意味がありません。

9.2.2 プロキシプロファイル

プロキシプロファイルを使用すると、複数のコンテンツフィルタリングポリシーを作成し、ネットワーク内のさまざまなアドレスに別々のポリシーを適用することができます。これにより、組織内のさまざまな部門に対して別々のポリシーを定義できます。さらに、各プロキシプロファイルには独自のユーザ認証方式を設定できます。

プロキシプロファイルを作成するには、次の手順に従います。

1. **「*新規プロキシプロファイル*」をクリックします。**
   「*プロキシプロファイルの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このプロファイルを説明する名前を入力してください。

   位置:プロキシプロファイルの優先順位を定義する位置番号。番号が小さいほど優先順位が高くなります。プロキシプロファイルは昇順に照合されます。あるプロキシプロファイルが一致すると、それ以降、それより大きい番号のプロキシプロファイルは評価されません。より詳細なプロファイルをリストの上部に配置することで、最も限定的でないプロファイルが最後に照合されるようになります。

   送信元ネットワーク:このプロキシプロファイルを使用するネットワークを選択します(これは必須フィールドです)。

   送信元エンドポイントグループ:このプロキシプロファイルを使用するエンドポイントグループを選択します。エンドポイントグループは「*エンドポイントプロテクション > コンピュータ管理 > グループ管理*」タブで作成するグループです。グループで「*Web コントロール*」が有効になっている場合、参照するエンドポイントマシンに*プロキシプロファイル*を適用できます。

   警告 – ここでは、他のプロキシプロファイルで使用されている送信元ネットワークおよびエンドポイントグループを選択しないでください。選択すると、コンテンツフィルタのアクション

とユーザ/グループのマッピングに不整合が生じ、特定のネットワークセグメントに属するユーザが、本来アクセスすべきではない Web サイトを閲覧できるようになる可能性があります。

フィルタ割当て:フィルタ割当てを選択します。フィルタ割当てとは 1セットの Web プロテクション構成設定であり、これを使用すると、さまざまなユーザ/グループにさまざまなレベルの保護をさまざまなタイミングで割当てることができます(詳しくは、「*Web プロテクション > Web フィルタリングプロファイル > フィルタ割り当て*」を参照してください)。複数のフィルタ割当てを選択することができます。さらに、どのフィルタ割当てを最初に適用するのかを指定することができます。これは、同じユーザまたはユーザグループに対して、さまざまなフィルタ割当てをさまざまなタイミングで適用したい場合に便利です。一般に、より詳細な割当てをリストの上部に配置することで、最も限定的でない割り当てが最後に照合されるようになります。これには、2つ以上のフィルタを選択すると表示される矢印アイコンを使用します。

注 – Web フィルタが「*基本ユーザ認証*」、「*Active Directory SSO*」、または「*eDirectory SSO*」モードで実行されている場合は、「*デフォルトフィルタ割当て*」を選択することもできます。この割当てでは、「*Web フィルタリング > グローバル*」タブで設定したユーザ/グループに「*デフォルトフィルタアクション*」が割当てられています。オペレーションモードを「*標準*」または「*透過*」に設定した場合でも、ユーザやグループが選択されたフィルタ割当てを使用することができますが、この場合、このプロキシプロファイルの使用時に、当該のユーザやグループは無視され、フィルタ割り当てに指定された期間定義のみが考慮されます。

フォールバックアクション:フォールバックアクションとは、会社のセキュリティポリシーを反映するための特別なフィルタアクションであり、選択されたフィルタ割当てがいずれも一致しない場合に、要求に適用されます。たとえば、厳格なセキュリティポリシーを遵守する必要がある場合、例外なくすべての Webトラフィックをブロックする特別なフィルタアクションをフォールバックとして作成することができます。また、ここで選択できる「*デフォルトフィルタアクション*」は、「*Webプロテクション > Web フィルタリング > URL フィルタリング*」タブでの設定に対応しています。

オペレーションモード:各プロキシプロファイルに対し、複数のユーザ認証方式から選択することができます。異なるプロキシプロファイルに異なる認証方式を持たせることができますが、1つのプロキシプロファイルには1つの認証方式しか使用できません。「*Web フィルタリング > グローバル*」タブで設定したオペレーションモード以外のオペレーションモードを選択することもできます。ただし、その認証が期待どおりに機能するのは、ここで選択した認証モー

ドがすべてのフィルタ割当てで使用されるすべてのユーザおよびグループオブジェクトの認証モードと一致している場合に限られます。次のオペレーションモードを使用できます。

- **標準:**標準モードでは、Web フィルタはデフォルトでクライアント要求をポート 8080 で待機し、「*許可ネットワーク*」ボックスにリストされたネットワーク内のすべてのクライアントに対して接続を許可します。このモードで使用する場合、クライアントはブラウザの設定で Web フィルタに HTTP プロキシを指定していることが必要です。
  認証タイプ:
  - **なし:**認証を行わない場合に選択します。
  - **Active Directory SSO:**「*定義とユーザ > 認証サーバ > サーバ*」タブで、「*Active Directory シングルサインオン*」(SSO)を設定した場合、これを選択します。これにより、NTLM ユーザ認証が認証クライアントで使用されます。動作が保証されるのは Internet Explorer のみです。このモードで使用する場合、クライアントはブラウザの設定で Web フィルタに HTTP プロキシを指定していることが必要です。

    注 – Active Directory ユーザグループを定義する際、LDAP 文字列でなく、Active Directory グループやユーザ名を手動で入力することで、「*Active Directory グループ*」ボックスに必要なエントリを追加することを強く推奨します。例:LDAP 文字列、`CN=ads_group1,CN=Users,DC=example,DC=com` の代わりに `ads_group1` という名前を入力してください。

    注 – Kerberos を使用している場合、「*Active Directory グループ*」ボックスには、グループのみを追加してください。エントリがユーザの場合、Web フィルタによって許可されていません。

  - **エージェント:**Sophos Authentication Agent (SAA)を使用する場合に選択します。Webフィルタを使用するためには、エージェントと認証を開始する必要があります。
  - **Apple OpenDirectory SSO:**「*定義とユーザ > 認証サーバ > サーバ*」タブで「*LDAP*」を設定しており、Apple OpenDirectory を使用している場合、これを選択します。さらに、プロキシが正しく機能するようにするためには、「*Web プロテクション > Web フィルタリング > 詳細*」タブで、MAC OS X シングルサインオン Kerberos 鍵ファイルをアップロードする必要があります。このモードで使用する場合、クライアントはブラウザの設定で Web フィルタに HTTP プロキシを指定していることが必要です。Safari ブラウザは SSO をサポートしていません。

- **基本ユーザ認証:**このモードでは、各クライアントは、プロキシを使用する前にこのプロキシに対して自己認証する必要があります。サポートされる認証方式について詳しくは、「*定義とユーザ > 認証サーバ*」を参照してください。このモードで使用する場合、クライアントはブラウザの設定で Web フィルタに HTTP プロキシを指定していることが必要です。
- **eDirectory SSO:**「*定義とユーザ > 認証サーバ > サーバ*」タブで「*eDirectory*」を設定した場合、これを選択します。このモードで使用する場合、クライアントはブラウザの設定で Web フィルタに HTTP プロキシを指定していることが必要です。

  注 – eDirectory および Active Directory のシングルサインオン(SSO)モードの場合、Web フィルタはアクセス先の IP アドレスと資格情報を最大 15分間キャッシュします。Apple OpenDirectory SSO の場合、キャッシュできるのはグループ情報のみです。これは、認証サーバへの負荷を軽減するために行われます。逆に言うと、ユーザ、グループ、またはアクセスしているユーザのログインステータスの変更が Web フィルタによって反映されるまで、最大 15 分かかります。

- **透過モード:**透過モードでは、ポート 80(SSL を使用している場合はポート 443)でクライアントブラウザアプリケーションが 行うすべての接続はインターセプトされ、クライアント側の設定なしでプロキシにリダイレクトされます。クライアントが Web フィルタサーバを意識することは全くありません。このモードの利点は、追加の管理やクライアント側での設定が不要であることで、短所は、処理できるのが HTTP (ポート80) 要求のみであることです。そのため、透過モードを選択すると、クライアントのプロキシ設定は無効になります。

  注 – 透過モードでは、Web フィルタは HTTP 要求から NTLM 認証ヘッダを削除します。さらに、Web フィルタはこのモードでは FTP 要求を処理できません。クライアントがこのようなサービスにアクセスする必要がある場合は、ファイアウォールでポート(21)を開く必要があります。一部の Web サーバは、ポート80 以外のポート経由でストリーミング動画や音声などのデータを送信します。これらの要求は、Web フィルタが透過モードで機能しているときは検知されません。このようなトラフィックにも対応したい場合には、他のモードを使用するか、これらを許可する明確なファイアウォールルールを入力する必要があります。

認証タイプ:

- **なし:**認証を行わない場合に選択します。
- **エージェント:**Sophos Authentication Agent（SAA）を使用する場合に選択します。Web フィルタを使用するためには、エージェントと認証を開始する必要があります。
- **ブラウザ:**選択すると、Web フィルタへの自己認証のためのログインダイアログがユーザのブラウザに表示されます。このモードでは、クライアント側のブラウザ設定なしで、ユーザ名に基づく追跡、報告、およびサーフィンが可能になります。さらに、そのダイアログウィンドウに追加で免責条項を表示することができます。この場合、ユーザが先に進むためには、免責条項に同意する必要があります。免責条項について詳しくは、「*管理 > カスタマイズ > Web メッセージ*」の章を参照してください。

フル透過モード（オプション）: クライアントの送信元 IP をゲートウェイの IP で置き換えず、そのまま維持する場合は、これを選択します。これは、クライアントがパブリック IP アドレスを使用しており、Web フィルタによって隠すべきではない場合に便利です。このオプションはブリッジモードのみで意味があるため、ブリッジモードでしか利用できません。

HTTPS（SSL）トラフィックのスキャン:HTTP トラフィックに加え HTTPS トラフィックもスキャンする場合は、このチェックボックスにチェックを入れます。

コメント（任意）:説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しいプロファイルが「*プロキシプロファイル*」リストに表示されます。

重要 – SSL スキャニングを透過モードと組み合わせて有効にすると、一部の SSL 接続（SSL VPN トンネルなど）が失敗します。SSL VPN 接続を有効にするには、対応するターゲットホストを「*透過モードスキップリスト*」に追加します（「*Web プロテクション > Web フィルタリング > 詳細*」を参照）。
さらに、自己署名証明書でホストにアクセスするには、「*証明書信頼性チェック*」オプションを選択して、これらのホストの除外を作成する必要があります。これにより、プロキシで証明書のチェックが行われません。

プロキシプロファイルを編集または削除するには、対応するボタンをクリックします。

9.2.3 フィルタ割当て

「*Web フィルタリングプロファイル > フィルタ割当て*」タブでは、特定のユーザおよびユーザグループにフィルタアクションを割り当てることができます。フィルタアクションでは、ブロックすべき Web サイトや Web サイトカテゴリを定義することによって「何を」に焦点をあてますが、フィルタ割り当てでは、これらのアクションを特定のタイミングでユーザとユーザグループに割り当てることによって「誰」と「いつ」に焦点をあてます。

注 –「*Web プロテクション > Web フィルタリング > ウイルス対策/マルウェア対策*」タブで行った各種設定（アンチウイルススキャン、ファイル拡張子フィルタ、MIME タイプフィルタ、コンテンツ削除）と「*URL フィルタリング*」タブで行った各種設定（カテゴリ、ブロックする URL）は、下の「*フィルタアクション*」ドロップダウンリストで選択できる「*デフォルトフィルタアクション*」として保存されます。

フィルタ割り当てを作成するには、次の手順に従います。

1. **「*新規フィルタ割り当て*」をクリックします。**
   「*新規フィルタ割り当ての作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前:この割当てを説明する名前を入力してください。

   許可ユーザ/グループ:特定のフィルタアクションを使用できるユーザとグループを選択します。新しいフィルタ割り当ては、ここで選択したユーザおよびグループと同じ認証モードを使用する Web フィルタプロファイルのみに追加する必要があります。

   タイムイベント:ファイアウォールルールやフィルタプロファイルを特定の時間範囲に制限するために使用できる単一の（または繰り返される）時間帯です。詳細は、「*定義とユーザ > 時間帯定義*」を参照してください。

   フィルタアクション:上で定義したユーザとユーザグループに割り当てるフィルタアクションを選択します。

   コメント（任意）:説明などの情報を追加します。
3. **「*保存*」をクリックします。**
   新しい割り当てが「*フィルタ割り当て*」リストに表示されます。

フィルタ割り当てを編集または削除するには、対応するボタンをクリックします。

Web フィルタプロファイルの作成時に、各フィルタ割り当てを選択できます。

9.2.4 フィルタアクション

「*Web フィルタリングプロファイル > フィルタアクション*」タブでは、一連の Web プロテクション構成設定を作成および編集できます。この設定を使用して、さまざまなタイプやレベルの保護をカスタマイズすることが可能です。フィルタアクションは、さまざまなユーザやユーザグループに割り当てることができ、Web アクセスをコントロールするための柔軟な手法となります。

フィルタアクションを作成するには、次の手順に従います。

1. **「*新規フィルタアクション*」をクリックします。**
   「*新規フィルタアクションの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このアクションを説明する名前を入力してください。

   モード:選択した Web サイトをブロックするか許可するかを選択します。次のオプションを使用できます。
   - **デフォルトで許可:**このオプションを選択すると、選択した Web サイトはブロックされますが、他のすべての Web サイトは許可されます。
   - **デフォルトでブロック:**このオプションを選択すると、選択した Web サイトを除くすべての Web サイトがブロックされます。

   レピュテーション: Web サイトは「*信頼される*」、「*中立*」、「*疑わしい*」のいずれかに分類できます。未分類の Web サイトを「*未確認*」と呼びます。ネットワークからアクセスできる Web サイトがどのような評判を持つべきかを決定することができます。選択したレピュテーションを下回る Web サイトはブロックされます。

   スパイウェア通信をブロック:このオプションを選択すると、サーバからクライアントへのトラフィックでスパイウェアを検出し、ブロックします。これにより、ネットワーク内のコンピュータが新しいスパイウェアに感染するのを防ぐことができます。さらに、この機能を有効にすると、すでにインストールされているスパイウェアアプリケーションについても検出し、トラフィックをブロックできます。この結果、スパイウェアが収集したユーザ情報がインターネットに送信されなくなります。このオプションは、モードを「*デフォルトでブロック*」に変更すると使用できません。

   ブロックする Web サイトカテゴリ:ブロックする Web サイトカテゴリを選択します。ここで選択する Web サイトカテゴリとその下位のサブカテゴリのマッピングは、「*Web プロテクション > Web フィルタリング > URL フィルタリングカテゴリ*」タブで変更できます。前述の「*モード*」を「*デフォ*

ルトでブロック」に設定した場合、このオプションは「*これらの Web サイトカテゴリを許可*」に変わります。

未分類サイトをブロック:このオプションを選択すると、未知のコンテンツのある Web サイトをブラウザで開くことができなくなります。この機能は、好ましくないと思われる Web サイトが相応の分類をされていない場合のフォールバックセキュリティメカニズムと考えることができます。前述の「*モード*」を「*デフォルトでブロック*」に設定した場合、このオプションは「*未分類のサイトを許可*」に変わります。

許可するURL/サイト:特定の URL や Web サイト、または特定のドメインにある複数の Web ページを、そのカテゴリに関わらずブロックするには、ここに入力します。その結果、ここで定義した Web サイトが、許可するカテゴリに属している場合でも、ブロックすることができます。URL 定義を追加するには、プラスアイコンをクリックして「*正規表現オブジェクトを追加*」ダイアログウィンドウを開き、以下のデータを入力します。

- **名前:**正規表現を説明する名前を入力してください。
- **ドメイン:**すべて、または特定の Web ページをブロックするドメインを入力します。ドメイン名全体を入力する必要があることに注意してください。たとえば、`www`も含める必要があります。以下で指定する正規表現のいずれか 1つがこの URL に一致した場合、指定したドメインの Web ページはブロックされます。正規表現を指定しなかった場合は、ドメイン全体がブロックされます。
- **正規表現:**上で指定したドメインの特定の Web ページをブロックするには、正規表現を入力します。上でドメインを指定しなかった場合は、この正規表現がすべてのドメインに適用されます。正規表現によっては、対象の URL だけではなく、検索結果や類似 URL の一部にも一致してしまうため、意図しないブロックにつながる可能性があります。

  参照 – Web フィルタリングで正規表現を使用する方法の詳細は、Sophos サポートデータベースを参照してください。

  注 – Web ページはできるだけ詳細に指定してください。ドメインを指定せずに正規表現のみを指定すると、意図しないブロックにつながる可能性があります。

- **コメント**(任意):説明などの情報を追加します。

前述の「*モード*」を「*デフォルトでブロック*」に設定した場合、このオプションは、「*許可する URL/サイト*」に変わります。

常に許可する URL/サイト:特定の URL や Webサイト、または特定のドメインにある複数の Web ページを、そのカテゴリやブロックリストに存在するかどうかに関わらず明示的に許可するには、ここに入力します。

「+」(プラス)アイコンをクリックして、「*正規表現オブジェクトを追加*」ダイアログウィンドウを開きます。上記のオプションの説明に従って、適切なデータを入力します。説明は、このオプションにも共通しています。

前述の「*モード*」を「*デフォルトでブロック*」に設定した場合、このオプションは、「*常にブロックする URL/サイト*」に変わります。

参照 – Web フィルタリングで正規表現を使用する方法の詳細は、Sophos サポートデータベースを参照してください。

セーフサーチ: Google、Bing、Yahoo の各検索エンジンに対して SafeSearch の使用を強制することができます。セーフサーチフィルタは、子供にふさわしくないコンテンツ(犯罪や不正)を検索結果から削除します。有効にすると、Web フィルタ経由で Web サーフィンをするユーザはフィルタをオフにできません。

YouTube for Schools:これを有効にすると、ユーザが再生できる YouTube 動画は、YouTube EDU サブセクションの YouTube 動画かユーザの学校のアカウントでアップロードされている YouTube 動画に制限されます。これが機能するためには、YouTube for Schools プログラムに登録して、スクール ID を取得し、それを以下に入力する必要があります。

注 – Sophos UTMでは、トップレベルドメインの `youtube.com` と `ytimg.com` に加え、一般的な動画がブロックされないことを確認する必要があります。

- **YouTube School ID:**「*YouTube for Schools*」を有効にした場合、スクール ID または YouTube から提供されたコードを入力する必要があります。

ブロック対象ファイル拡張子:ファイル拡張子を指定すると、拡張子に基づいて特定タイプのファイルをブロックすることができます(実行可能形式のバイナリなど)。ファイル拡張子を追加するには、「*ブロックするファイル拡張子*」ボックスのプラスアイコンをクリックし、ブロックしたい拡張子(`exe` など)を入力します。区切り記号のドットは不要です。

ブロック対象 MIME タイプ:ブロックする MIME タイプを追加するには、「*ブロック対象 MIME タイプ*」ボックスの「+」アイコンをクリックし、MIME タイプを入力します(例: `image/gif` など)。

コンテンツ削除:これを選択すると、「*JavaScript を削除*」オプションと「*埋め込みを削除*」オプションが表示されます。これらのオプションを使用して、<SCRIPT> タグと <OBJECT> タグを HTML ページから削除するか否かを設定できます。「JavaScript を削除」オプションを使用すると、HTML ページに埋め込まれた(または HTML ページからインクルードされた) JavaScript が無効になり、「埋め込みを削除」を使用すると、受信側 HTTP/S トラフィックから ActiveX、Flash、Java アプレットなどの動的コンテンツが除外されます。動的コンテンツを埋め込む方法は他にもあるので、特定のコンテンツを確実に除外するには、「*ブロック対象 MIME タイプ*」ボックスで指定してください。

アンチウイルススキャンを使用:このオプションを選択すると、受信側 Web トラフィックに悪質なコンテンツが含まれていないかスキャンが行われます。Sophos UTM は、最高のセキュリティを実現するさまざまなアンチウイルスエンジンを備えています。

最大スキャンサイズ:アンチウイルスエンジンでスキャンする最大ファイルサイズを指定します。このサイズを超えるファイルはスキャン対象外となります。

許可するダウンロードの最大サイズ:指定したサイズ(MB)を超えるファイルのダウンロードを禁止する場合にこのオプションを指定します。

労働協議会の会員など、活動内容を記録することが禁止されているユーザがいる場合には、次の 2つのオプションが便利です。

- **アクセスしたページをログに記録する:**チェックを外すと、アクセスしたページがログやレポートから除外されます。
- **ブロックされたページをログに記録する:**チェックを外すと、ブロックしたページがログやレポートから除外されます。

親プロキシ:1つ以上の親プロキシの使用を設定できます。ボックスが空の場合、まず、「*親プロキシ*」タブに親プロキシの定義を作成してください。各プロキシの前にあるチェックボックスにチェックを入れて、親プロキシの使用を有効化します。複数のプロキシを選択した場合、「並び替え」アイコンを使用してプロキシを並べ替えることができます。選択した親プロキシは、最初のプロキシが一致するまで、所定の順序で適用されます。処理順序は位置番号によって決まるため、位置番号によってプロキシの順序を変更すると、処理順序も変わります。

3. **「*保存*」をクリックします。**
   新しいフィルタアクションが「*フィルタアクション*」リストに表示されます。

フィルタアクションを編集または削除するには、対応するボタンをクリックします。

フィルタ割り当てまたは Web フィルタプロファイルの作成時に、各フィルタアクションを選択できます。

注 – ここでは、「*デフォルトのコンテンツフィルタブロックアクション*」も参照できます。デフォルトでは、「*Web フィルタリング*」メニューの他のすべてのフィルタアクションや設定と一致しない HTTP/S リクエストがすべてブロックされます。

9.2.5 親プロキシ

親プロキシは、多くの場合、政府承認のプロキシサーバを通してインターネットアクセスをルーティングする必要のある国などで必要とされます。「*Web プロテクション > Web フィルタリングプロファイル > 親プロキシ*」ページでは、親プロキシの使用を、プロファイルに基づいて設定するかグローバルに設定できます。親プロキシをプロファイルで使用するためには、常に、このページで(あるいは「*Web フィルタリング > 詳細*」ページで)最初に設定する必要があります。

注 – 技術的な理由から、親プロキシを有効化した場合は、SSL スキャニングを有効にした状態での透過モードでの HTTPS 要求は行えません。

親プロキシを設定するには、次の手順に従います。

1. **「*新規親プロキシ*」をクリックします。**
   「*新規親プロキシ作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前:この親プロキシを説明する名前を入力してください。

   コメント(任意):説明などの情報を追加します。

   プロキシを使用するホスト:親プロキシを使用するホストをこのボックスに追加します(例: `*.wikipedia.org`)。ここではパターンマッチを使用できます。ただし、正規表現は使用できません。ボックスを空にすると、「*保存*」をクリックするとアスタリスク(*)が自動的に追加され、すべてのホストに該当します。従って、このようなプロキシ定義は、一致するプロキシが存在しない場合のフォールバックプロキシとみなされます。

   親プロキシ:親プロキシのネットワーク定義を選択または追加します。

   ポート:親プロキシ接続のデフォルトポートは 8080 です。親プロキシで別のポートを使用する場合、ここで変更できます。

   プロキシ認証が必要:親プロキシが認証を必要とする場合は、チェックボックスにチェックを入れ、表示されるテキストボックスにユーザ名とパスワードを入力します。
3. **「*保存*」をクリックします。**
   新しい親プロキシが「*親プロキシ*」リストに表示されます。

これで、このプロキシをフィルタアクションで使用することも、グローバルに使用することもできます。

親プロキシを編集または削除するには、対応するボタンをクリックします。

9.3 アプリケーションコントロール

UTMのアプリケーションコントロール機能を使用すると、トラフィックの種類に基づいてネットワークトラフィックをシェーピングおよびブロックすることができます。UTMの Web フィルタリング機能（「Web フィルタリング」の章を参照）と違い、アプリケーションコントロール分類エンジンを使用すると、ネットワークトラフィックを、プロトコルや URL 単位ではなく、よりきめ細かい基準で識別することができます。これは、Web トラフィックに関して特に便利です。Web サイトへのトラフィックは、通常ポート80で HTTP プロトコルを使用するか、ポート443で HTTPS プロトコルを使用しています。特定の Web サイト（facebook.com など）へのトラフィックをブロックしたい場合、Web サイトの URL（Web フィルタリング）に基づいてブロックすることができます。あるいは、ネットワークトラフィック分類を利用して、あらゆるURLから独立して facebook トラフィックをブロックすることができます。

UTMの分類エンジンは、ネットワークトラフィックの分類にレイヤ 7 パケット検査を使用します。

アプリケーショ制御は 2つの方法で使用できます。最初のステップでは、「*ネットワーク可視化*」ページでアプリケーションコントロール全般を有効にする必要があります。これにより、アプリケーションが一定の範囲で「可視化」されます。これをこのまま（または、特定の時間だけ）残し、ユーザに使用されているアプリケーション（フローモニタ、ロギング、レポーティングなど）を確認することができます。2 番目のステップでは、特定のアプリケーションをブロックし、他のアプリケーションは許可することができます。これには、「*アプリケーションコントロールルール*」ページで作成するルールを使用します。さらに、トラフィックシェーピングを使用して、定義したアプリケーションのトラフィックに特権を与えることができます。この設定は、Sophosの QoS 機能で行います。

9.3.1 ネットワーク可視化

「*Web プロテクション > アプリケーションコントロール > ネットワーク可視化*」ページでは、アプリケーションコントロールを有効または無効にすることができます。

アプリケーションコントロールを有効にすると、すべてのネットワークトラフィックが、その分類に応じて分類・ログされます。現在のネットワークトラフィックは、フローモニタに、タイプに関する詳細な情報と共に表示されます（「*フローモニタ*」の章を参照）。たとえば、HTTPトラフィックに関する情報は、おおもとのアプリケーション（「twitter」、「facebook」など）までドリルダウンされます。フローモニタを開くには、「*フローモニタ*」セクションで該当のインタフェースを選択し、「*フローモニタを開く*」ボタンをクリックします。

ログとレポートでは、ネットワークトラフィックとその分類に関する幅広い情報と、これらのアプリケーションを使用するクライアントとサーバの情報が表示されます。ログとレポートについて詳しくは、「*ログとレポート*」の章で、「*ログファイルの閲覧*」セクションを参照するか(ログ)、「*ネットワーク使用率 > 帯域使用状況*」セクションおよび「*Web プロテクション > アプリケーションコントロール*」セクションを参照してください(レポート)。

9.3.2 アプリケーションコントロールルール

「*Web プロテクション > アプリケーションコントロール > アプリケーションコントロールルール*」ページでは、ネットワークに対してトラフィックをブロックするか、または明示的に許可するアプリケーションを定義するネットワークトラフィック分類に基づいて、ルールを作成することができます。

デフォルトでは、アプリケーションコントロールを有効にするとすべてのネットワークトラフィックが許可されます。

アプリケーションコントロールルールの作成は、このページでもフローモニタでも可能です。フローモニタの方が使いやすいですが、ルールを作成できるのは、ネットワークで現在モニタリングされているトラフィックに対してのみです。

アプリケーションコントロールルールを作成するには、以下の手順に従います。

1. **「*アプリケーションコントロールルール*」タブで、「*新規ルール*」をクリックします。**
   「*新規ルール作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前(オプション):ルールの名前を入力します。フィールドを空のままにすると、システムがルールの名前を生成します。

   グループ:「*グループ*」オプションは、複数のルールを論理的にグループ化するのに便利です。リストの上部のドロップダウンリストを使用して、グループごとにルールをフィルタリング表示できます。グループ化は表示用のみで、ルールの一致には関係ありません。新しいグループを作成するには、「*<<新規グループ>>*」エントリを選択し、グループを説明する名前を「*名前*」に入力します。

   優先順位:優先順位番号。これによってルールの優先順位が定義されます。番号が小さいほど優先順位が高くなります。ルールは昇順に照合されます。あるルールが一致すると、それ以降、それより大きい番号のルールは評価されません。

   アクション:トラフィックをブロックするか許可するかを選択します。

   制御基準:アプリケーションタイプに基づいてトラフィックをコントロールするか、カテゴリに基づくダイナミックフィルタによってコントロールするかを選択します。

- **アプリケーション:**トラフィックは、アプリケーションに基づいてコントロールされます。「*制御するアプリケーション*」ボックスでアプリケーションを1つ以上選択します。
- **ダイナミックフィルタ:**トラフィックは、カテゴリに基づいてコントロールされます。「*制御するカテゴリ*」ボックスで分類を1つ以上選択します。

管理対象アプリケーション/カテゴリ:「フォルダ」アイコンをクリックして、アプリケーション/カテゴリを選択します。ダイアログウィンドウが開きます。これについては、次のセクションで詳しく説明します。

注 – 一部のアプリケーションはブロックすることができません。これは、Sophos UTMの適切なオペレーションのために必要です。このようなアプリケーションは、「*アプリケーション選択*」ダイアログウィンドウのアプリケーションテーブルでチェックボックスがオフになっています。たとえば、*WebAdmin*、*Teredo*、*SixXs*(IPv6トラフィック用)、*Portal*(ユーザポータルのトラフィック用)などが該当します。ダイナミックフィルタを使用すると、これらのアプリケーションのブロックも自動的に制限されます。

生産性(*ダイナミックフィルタのみ*):選択した生産性スコアが反映されます。

リスク(*ダイナミックフィルタのみ*):選択したリスクスコアが反映されます。

対象ネットワーク:このルールによってネットワークトラフィックを制御するネットワークまたはホストを選択するか、このボックスに追加します。これは、送信元ホスト/ネットワークにのみ適用されます。

ログ:このオプションはデフォルトでオンになっており、ルールと一致するトラフィックのロギングが有効になります。

コメント(任意):説明などの情報を追加します。

3. **「保存」をクリックします。**
新しいルールが「*アプリケーションコントロールルール*」リストに表示されます。

「アプリケーションまたはカテゴリの選択」ダイアログウィンドウ

アプリケーションコントロールルールを作成する際は、「*管理するアプリケーション(カテゴリ)を1つ以上選択してください*」というダイアログウィンドウからアプリケーションまたはアプリケーションカテゴリを選択する必要があります。

ダイアログウィンドウの下部に表示されるテーブルには、選択可能なアプリケーションまたは定義したカテゴリに属するアプリケーションが表示されます。デフォルトでは、すべてのアプリケーションが表示されます。

ダイアログウィンドウの上部には、テーブルに表示されるアプリケーション数を制限するための 3つの設定オプションがあります。

- **カテゴリ:**アプリケーションはカテゴリ別にグループ化されています。このリストには、利用可能なすべてのカテゴリが表示されます。デフォルトでは、すべてのカテゴリが選択されています。つまり、下部に表示されるテーブルには、利用可能なすべてのアプリケーションが表示されます。表示されるアプリケーションを特定のカテゴリに絞り込むには、クリックしてカテゴリリストを開き、1つ以上のカテゴリを選択します。
- **生産性:**アプリケーションは、生産性への影響(つまり生産性にこのアプリケーションが与える影響の度合い)によっても分類されています。例:一般的なビジネスソフトウェアの Salesforce のスコアは 5です。つまり、これを使用することで生産性が向上します。一方、オンラインゲームの Farmville のスコアは 1 で、これを使用すると生産性が低下します。ネットワークサービス DNS のスコアは 3 で、生産性への影響は中立的です。
- **リスク:**アプリケーションは、使用時のリスク(マルウェア、ウイルス感染、攻撃)によっても分類されています。数値が高いほど、リスクも高くなります。

ヒント – それぞれのアプリケーションには情報アイコンがあり、クリックすると各アプリケーションの説明が表示されます。テーブルヘッダのフィルタフィールドを使用して、テーブル内を検索することができます。

次に、「*新規ルール作成*」ダイアログボックスで選択したコントロールのタイプに応じて、以下を行います。

- ダイナミックフィルタで管理する場合:「*適用*」をクリックして、選択したアプリケーションをルールに適用します。
- アプリケーションで管理する場合:テーブルで、アプリケーションの前にあるチェックボックスをクリックし、管理対象のアプリケーションを選択します。「*適用*」をクリックして、選択したアプリケーションをルールに適用します。

「*適用*」をクリックするとダイアログウィンドウが閉じ、アプリケーションルールの設定の編集を続けることができます。

9.3.3 詳細

「*Web プロテクション > アプリケーションコントロール > 詳細*」ページでは、アプリケーションコントロールの詳細オプションを設定できます。

Sophos UTM AppAccuracy プログラム

Sophos UTM AppAccuracy プログラムに参加すると、ネットワークの可視性とアプリケーションコントロールの認識と分類の向上に貢献いただけます。このシステムは、匿名のアプリケーションフィンガープリントという形でデータを収集し、Sophosのリサーチチームへ送信します。ここでは、指紋を使用して、未分類のアプリケーションを識別し、ネットワーク可視化およびアプリケーションコントロールライブラリを改良および拡張します。

アプリケーションコントロールスキップリスト

このボックスにリストされているホストとネットワークは、アプリケーションコントロールの監視対象とはならないため、アプリケーションコントロールで管理することも、サービス品質のアプリケーションセレクタで管理することもできません。これは、送信元および宛先ホスト/ネットワークの両方に適用されます。

9.4 FTP

「*Web プロテクション > FTP*」タブでは、FTP プロキシを設定できます。*FTP (File Transfer Protocol)* は、インターネット上でのファイルのやり取りに幅広く使用されているプロトコルです。Sophos UTM は、ネットワークを通過するすべての FTP トラフィックの仲介役となるプロキシサービスを提供します。FTP プロキシには、FTP トラフィックのウイルススキャンや、FTP プロトコル経由で転送される特定のファイルタイプのブロックといった便利な機能が用意されています。

FTP プロキシは透過的に機能できます。つまり、ネットワーク内のすべての FTP クライアントは、最終宛先ではなくプロキシへの接続を確立します。続いて、クライアントから見えない状態でプロキシが要求に代わって新しいネットワーク接続を開始します。このモードのメリットは、その他の管理やクライアント側の設定が必要ないということです。

9.4.1 グローバル

「*Web プロテクション > FTP > グローバル*」タブでは、FTP プロキシの基本設定を構成できます。

FTP プロキシを設定するには、次の手順に従ってください。

1. **「グローバル」タブで、FTP プロキシを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*FTP 設定*」エリアが編集可能になります。

2. **許可するネットワークを選択します。**
   FTP プロキシの使用を許可するネットワークを選択します。
3. **オペレーションモードを選択します。**
   FTP プロキシのオペレーションモードを選択します。次のモードを使用できます。
   - **透過:**プロキシは、クライアントの要求をターゲットサーバに転送し、コンテンツをスキャンします。クライアント側での設定は不要です。
   - **非透過:**このモードを使用する場合、FTP クライアントを設定する必要があります。ゲートウェイの IP アドレスとポート 2121 を使用します。
   - **両方:**このモードを使用すると、一部のクライアントには透過モードを、他のクライアントには非透過モードを使用することができます。非透過モードで機能させるFTPクライアントを、ゲートウェイの IP アドレスとポート 2121 でプロキシを使用するように設定します。
4. **「*適用*」をクリックします。**
   設定が保存されます。

注 – FTP プロキシは、Active Directory 認証を使用する FTP サーバとは通信できません。FTP クライアントがこのような FTP サーバに接続できるようにするには、このサーバをFTP プロキシのスキップリストに追加します。スキップリストの設定は、「*詳細*」タブで行います。

9.4.2 ウイルス対策

「*Web プロテクション > FTP > ウイルス対策*」タブには、ウイルス、ワーム、その他のマルウェアなどの有害で危険なコンテンツを伝送する FTP トラフィックに対して講じることができるあらゆる対策が含まれています。

アンチウイルススキャンを使用:このオプションを選択すると、FTP 受信トラフィック全体がスキャンされます。Sophos UTMは、最高のセキュリティを実現するさまざまなアンチウイルスエンジンを備えています。

- **シングルスキャン:**デフォルト設定。「*スキャン設定*」タブに定義されたエンジンを使用して最高レベルのパフォーマンスを実現します。
- **デュアルスキャン:**各トラフィックに対し、異なるウイルススキャナを使用してスキャンを 2回行うことにより、検出率を最大限に高めます。ベーシックガードサブスクリプションではデュアルスキャンは利用できません。

最大スキャンサイズ:アンチウイルスエンジンでスキャンする最大ファイルサイズを指定します。このサイズを超えるファイルはスキャン対象外となります。

設定を保存するには「*適用*」をクリックします。

注 – ZIP ファイルなど、アーカイブされたファイルを悪意あるコンテンツについてスキャンすることはできず、ウイルススキャナを通過します。アーカイブされたファイルに含まれるマルウェアからネットワークを保護するには、該当するファイル拡張子をブロックすることを考慮してください。

ファイル拡張子フィルタ

この機能では、ファイルの拡張子（実行可能バイナリなど）に基づいて、「*ブロック対象ファイル拡張子*」ボックスにファイル拡張子がリストされているタイプのファイルを伝送する FTP 転送を Web トラフィックからフィルタします。ファイル拡張子を追加したり、ブロック対象から外すファイル拡張子を削除したりすることができます。ファイル拡張子を追加するには、「*ブロック対象ファイル拡張子*」ボックスのプラスアイコンをクリックし、ブロックする拡張子（exe など）を入力します。区切り記号のドットは不要です。設定を保存するには「*適用*」をクリックします。

9.4.3 除外

「*FTP > 除外*」タブでは、FTP プロキシの提供する選択可能なセキュリティオプションから除外するホワイトリストのホスト/ネットワークを定義することができます。

除外ルールを作成するには、次の手順に従います。

1. **「*除外*」タブで、「*新規除外リスト*」をクリックします。**
   「*除外リストを作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:この除外ルールを説明する名前を入力してください。

   実行しないチェック:スキップするセキュリティチェックを選択します。

   - **アンチウイルス:**選択すると、ウイルスやトロイの木馬などの好ましくないコンテンツがトラフィックに含まれていないかチェックするウイルススキャンが無効になります。
   - **拡張子ブロック:**選択すると、ファイル拡張子フィルタが無効になります。このフィルタは、ファイル拡張子に基づいてファイル転送をブロックするために使用します。
   - **許可サーバ:**選択すると、「*詳細*」タブで設定する許可サーバのチェックが無効になります。このオプションを選択すると、指定したクライアントホスト/ネットワークはすべての FTP サーバにアクセスできるようになります。また、指定したサーバホスト/ネットワークはすべてのクライアントにアクセスできるようになります。

クライアントホスト/ネットワークで除外:このオプションを選択すると、「*クライアントホスト/ネットワーク*」ボックスが開きます。この除外ルールのセキュリティチェックから除外するクライアントホスト/ネットワークを選択します。

サーバホスト/ネットワークで除外:このオプションを選択すると、「*サーバホスト/ネットワーク*」ボックスが開きます。この除外ルールのセキュリティチェックから除外するサーバホスト/ネットワークを選択します。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しい除外が「*除外*」リストに表示されます。

除外ルールを編集または削除するには、対応するボタンをクリックします。

9.4.4 詳細

「*FTP > 詳細*」タブでは、FTP プロキシの透過モードをスキップできるホストとネットワークを指定できます。さらに、アクセスを許可する FTP サーバを定義できます。

FTP プロキシスキップリスト

ここにリストされたホストとネットワーク(FTP クライアントおよび FTP サーバ)は、FTP トラフィックの透過的なインターセプションから除外されます。ただし、これらのホストおよびネットワークで FTP トラフィックを許可するには、「*リスト内のホスト/ネットワークの FTP トラフィックを許可*」チェックボックスにチェックを入れます。このチェックボックスにチェックを入れない場合は、ここでリストされているホストとネットワークに特定のファイアウォールルールを定義する必要があります。

注 – FTP プロキシは、Active Directory 認証を使用する FTP サーバとは通信できません。FTP クライアントがこのような FTP サーバに接続できるようにするには、このサーバを FTP プロキシのスキップリストに追加します。

FTP サーバ

ホスト/ネットワークからのアクセスを許可する FTP サーバまたはネットワークを選択または追加します。一部の FTP クライアントや FTP サーバがこのリストをバイパスするように、「*除外*」タブで除外ルールを作成できます。

10 Eメールプロテクション

この章では、Sophos UTMの基本的なメールプロテクション機能を設定する方法を説明します。WebAdmin の「*Eメールプロテクション統計*」ページには、メール送信者、メール受信者、スパム送信元（国別）、検知数によるマルウェアのその日の上位 10件までに加え、同時接続の概要が表示されます。各セクションには「*詳細*」リンクがあります。リンクをクリックするとWebAdmin の該当するレポートセクションが表示され、詳細な統計情報を参照できます。

この章では、次のトピックについて説明します。

- SMTP
- SMTP プロファイル
- POP3
- 暗号化
- 隔離レポート
- メールマネージャ

10.1 SMTP

「*Eメールプロテクション > SMTP*」メニューで SMTP プロキシを設定できます。SMTP は *簡易メール転送プロトコル (Simple Mail Transfer Protocol)* の略で、メールをメールサーバに転送するために使用されるプロトコルです。Sophos UTMは SMTP のためのアプリケーションレベルのゲートウェイを装備しており、これを使用して内部メールサーバをリモートの攻撃から守り、さらに強力なウイルススキャンおよびメールフィルタサービスを提供できます。

注 – SMTP プロキシを正しく使用するには、有効なネームサーバ（DNS）を設定する必要があります。

10.1.1 グローバル

「*Eメールプロテクション > SMTP > グローバル*」タブで、SMTP 設定に対して「*シンプルモード*」を使用するか「*プロファイルモード*」を使用するかを決定できます。

1. **SMTPを有効にします。**
   トグルスイッチをクリックします。

トグルスイッチが緑色になり、「*設定モード*」エリアが編集可能になります。

2. **設定モードを選択します。**
シンプルモード:すべてのドメインが同じ設定を共有している場合はこのモードを使用します。ただし、ドメイン名、メールアドレス、およびホストに基づいて除外ルールを定義することもできます。これは「*プロファイルモード*」と異なり機能的な制限はありません。

プロファイルモード:(ベーシックガードサブスクリプションでは、利用できません。)このモードでは、個々のドメインあるいはドメイングループのアンチスパムやアンチウイルスなどのグローバル設定を、「*SMTPプロファイル*」メニューでそれらのプロファイルを作成することで、上書きまたは拡張できます。「*SMTP*」メニューで行った設定は、依然として指定のドメインに適用され、プロファイルのデフォルトとなります。「*プロファイルモード*」には、UTMのプロファイルモードや動作の推奨設定について、いくつかの注意事項があります。

3. **「*適用*」をクリックします。**
選択したモードが有効になります。

10.1.2 ルーティング

「*ルーティング*」タブで、SMTP プロキシのドメインとルーティングターゲットを設定し、受信者の検証方法を定義します。

SMTP プロキシのルーティングを設定するには、以下の手順に従います。

1. **内部ドメインを入力します。**
メールのドメインを入力するには、「*ドメイン*」ボックスの「+」アイコンをクリックします。

表示されたテキストボックスに、`example.com` の形式でドメインを入力し、「*適用*」をクリックします。すべてのドメインがリストされるまでこのステップを繰り返します。

プロファイルモード:グローバル設定を使用するドメインのみを入力します。他のすべてのドメインは、それぞれのプロファイルにリストします。

2. **内部サーバを指定します。**
「*ルート毎*」ドロップダウンリストで、上記でリストしたドメイン宛てのメールの転送先ホストを選択します。一般的なターゲットホストとしては、ローカルネットワーク上の Microsoft Exchange Server が挙げられます。さまざまなサーバタイプから選択できます。

   - **スタティックホストリスト:**「*ホストリスト*」ボックスで、ターゲットルートのホスト定義を選択します。基本的なフェイルオーバー用に複数のホスト定義を選択できます。最初のホストへの配信に失敗すると、メールは次のホストにルーティングされます。ただし、ホストのスタティック(静的)な順序は、現在のバージョンのSophos UTMでは決定

できず、やや偶発的に決定されます。基本的な負荷分散機能をさらに効率よく達成できるようにホストグループへの配信をランダム化するには、「*DNS ホスト名*」ルートタイプを使用し、複数の A レコードを持つホスト名を指定します(*A レコード*または*アドレスレコード*は、ホスト名を IP アドレスにマップします)。

- **DNS ホスト名:**ターゲットルートの*完全修飾ドメイン名*(FQDN)を指定します(例: `exchange.example.com`)。複数の A レコードを持つ DNS 名を選択すると、各サーバへのメールはランダムに配信されます。さらに、1台のサーバに障害が発生すると、そのサーバ宛てのすべてのメールは残りのサーバに自動的にルーティングされます。
- **MX レコード:**MX レコードを使用して、お使いのドメインにメールをルーティングすることもできます。このルートタイプを選択すると、Sophos UTMのメール転送エージェントは、受信者のドメイン名(メールアドレスの "@" 文字に続く部分)の MX レコードを要求する DNS クエリを行います。ゲートウェイが上記で指定したドメインのプライマリ MX ではないことを確認する必要があります。なぜなら、自らにはメールを配信しないからです。

3. **「*適用*」をクリックします。**
   設定が保存されます。

受信者の確認

受信者検証:ここでメール受信者を確認するかどうかと確認方法を指定できます。

- **コールアウト使用:**受信者検証の要求がサーバに送信されます。
- **Active Directory 使用:**受信者検証の要求が Active Directory サーバに送信されます。Active Directory を使用するには、「*定義とユーザ > 認証サーバ > サーバ*」で指定された Active Directory サーバを備えていることが必要です。ベース DNを「*代替ベース DN*」フィールドに入力します。

  注 – Active Directory 受信者検証を使用すると、サーバが応答しない場合にメッセージがバウンスされる場合があります。

- **オフ:**受信者検証は完全にオフにできますが、推奨されません。なぜなら、オフにすると、スパムトラフィックが増大して、辞書攻撃の危険性が高まるからです。この結果、隔離場所が迷惑メールで溢れてしまうことになります。

設定を保存するには「*適用*」をクリックします。

10.1.3 ウイルス対策

「*ウイルス対策*」タブには、ウイルス、ワーム、その他のマルウェアなどの有害で危険なコンテンツを含むメールに対するさまざまな対策が含まれています。

注 – 送信メールは、「*リレー*」タブの「*リレー(送信)メッセージのスキャン*」が選択されている場合にスキャンされます。

SMTP トランザクション時にスキャン

「*SMTP トランザクション時にマルウェアをリジェクト*」チェックボックスにチェックを入れることで、SMTP トランザクション中にスキャンを行い、マルウェアが含まれている場合は拒否することができます。

プロファイルモード:この設定はプロファイルごとには変更できません。1人以上の受信者がいるメッセージで、受信者の 1人のプロファイルで「*アンチウイルススキャン*」がオフになっている場合は、この機能はスキップされます。したがって、以下の通常のアンチウイルス設定を「*ブラックホール*」あるいは「*隔離*」のいずれかの設定にしておくことをお勧めします。

設定を保存するには「*適用*」をクリックします。

アンチウイルススキャン

このオプションでは、ウイルス、トロイの木馬、疑わしいファイルタイプなどの不要なコンテンツがないかどうか、メールをスキャンします。悪意のあるコンテンツを含むメッセージはブロックされて、メールの隔離場所に保存されます。ユーザは、Sophosユーザポータル またはデイリーの隔離レポートで、隔離されたメッセージを確認してリリースできます。ただし、悪意のあるコンテンツを含むメッセージは、メールマネージャで管理者のみが隔離からリリースできます。

アンチウイルス:悪意あるコンテンツを含むメッセージの処理方法を設定できます。次の作業を実行できます。

- **オフ**:アンチウイルススキャンを実行しません。
- **ブラックホール**:メッセージは受信後、ただちに削除されます。送信メッセージは、意図しないメールの紛失を回避するために、ブラックホール化されることがありません。代わりに、隔離されます。
- **隔離**:メッセージはブロックされ、メールの隔離場所に保存されます。隔離されたメッセージは、ユーザポータルまたはデイリーの隔離レポートで確認できます。悪意のあるコンテンツを含むメッセージを隔離場所からリリースできるのは、管理者だけです。

Sophos UTM は、最高のセキュリティを実現するさまざまなアンチウイルスエンジンを備えています。

- **シングルスキャン:**デフォルト設定。「*スキャン設定*」タブに定義されたエンジンを使用して最高レベルのパフォーマンスを実現します。
- **デュアルスキャン:**各トラフィックに対し、異なるウイルススキャナを使用してスキャンを 2回行うことにより、検出率を最大限に高めます。ベーシックガードサブスクリプションではデュアルスキャンは利用できません。

スキャンできないコンテンツ、暗号化されたコンテンツの隔離:このオプションを選択して、コンテンツをスキャンできなかったメールを隔離します。スキャンできないコンテンツは、暗号化されたもの、破損したアーカイブ、またはサイズが大きすぎるコンテンツの他、スキャナの不具合などの技術的な問題による場合があります。

設定を保存するには「*適用*」をクリックします。

MIME タイプフィルタ

MIME タイプのフィルタは MIME タイプのメールコンテンツを読みます。さまざまな MIME タイプをどう取り扱うかを定義できます。

- **音声コンテンツを隔離:**このチェックボックスにチェックを入れると、mp3 あるいは wav ファイルなどの音声コンテンツが隔離されます。
- **動画コンテンツを隔離:**このチェックボックスにチェックを入れると、mpg あるいは mov ファイルなどの動画コンテンツが隔離されます。
- **実行可能ファイルコンテンツを隔離:**このチェックボックスにチェックを入れると、exe ファイルなどの実行可能ファイルコンテンツが隔離されます。

隔離する他のタイプ:上記以外の MIME タイプを隔離するには、「*隔離する他のタイプ*」ボックスの「+」アイコンをクリックし、MIME タイプ(例: `image/gif`)を入力します。スラッシュ右側にワイルドカード(`*`)を使用できます(例: `application/*`)。

ホワイトリスト化するタイプ:このボックスを使用して一般的に信頼できる MIME タイプを許可します。MIME タイプを追加するには「*ホワイトリスト化するタイプ*」ボックスの「+」アイコンをクリックし、MIME タイプを入力します。設定を保存するには「*適用*」をクリックします。

MIME タイプ	MIME タイプのクラス
audio/*	音声ファイル
video/*	動画ファイル

MIME タイプ	MIME タイプのクラス
application/x-dosexec	アプリケーション
application/x-msdownload	
application/exe	
application/x-exe	
application/dos-exe	
vms/exe	
application/x-winexe	
application/msdos-windows	
application/x-msdos-program	

Table 2: MIMEタイプフィルタで認識されるMIMEタイプ

ファイル拡張子フィルタ

この機能は、ファイル拡張子に基づいて特定タイプのファイル（実行可能ファイルなど）を含むメールを（警告付きで）フィルタリングし、隔離します。ファイル拡張子を追加するには、「*ブロック対象ファイル拡張子*」ボックスの「+」アイコンをクリックし、禁止するファイル拡張子（例: `exe` または `jar`（区切り文字のドットなし））を入力します。設定を保存するには「*適用*」をクリックします。

ヒント – 禁止されたファイル拡張子に対してアーカイブを検索することはできません。アーカイブに含まれるマルウェアからネットワークを保護するには、該当するアーカイブのファイル拡張子をブロックすることを考慮してください。

アンチウイルスチェックフッタ

各送信メールで、悪意あるコンテンツについてメールをスキャン済みであることをユーザに知らせる特別なフッタを追加してカスタマイズできます。ただし、「*リレー*」タブの「*リレー（送信）メッセージのスキャン*」チェックボックスが選択されている場合にのみフッタが追加されます。さらに、ウイルス対策チェックフッタは、返信メールの場合（*In-Reply-To* ヘッダを持つもの）、またはメールのコンテンツタイプを判定できない場合は、メールに追加されません。設定を保存するには「*適用*」をクリックします。

注 – メールクライアント(例: Microsoft Outlook または Mozilla Thunderbird)が署名済みまたは暗号化済みのメッセージにフッタを追加すると、署名が破壊されて無効になります。デジタル署名をクライアント側で作成する場合は、アンチウイルスチェックフッタオプションを無効にしてください。ただし、メール通信のプライバシーや認証を保ちながら、一般的なウイルス対策チェックフッタを使用する場合は、Sophos UTM の組み込みメール暗号化機能の使用を考慮してください。ゲートウェイ上でのメール暗号化では、デジタル署名を作成する前にフッタがメッセージに付加されるため、署名が損なわれることはありません。

10.1.4 スパム対策

Sophos UTM Sophos UTM を設定して、未承諾のスパムメールを検出したり、既知の(または疑わしい)スパム発信者からのスパム送信を識別することができます。「*スパム対策*」タブにある設定オプションを使用して、SMTP のセキュリティ機能を設定し、未承諾の宣伝用メールなどからネットワークを保護します。

注 – 送信メールは、「*リレー*」タブの「*リレー(送信)メッセージのスキャン*」が選択されている場合にスキャンされます。

注 – このタブの一部の機能は、ベーシックガード サブスクリプションでは利用できません。

SMTP トランザクション中のスパム検出

SMTP トランザクション中にスパムを拒否することができます。「*SMTP 上でリジェクト*」オプションに、次のいずれかの設定を選択します。

- **オフ**:スパム検出は無効となり、スパムが原因でメールが拒否されることは一切ありません。
- **Confirmed Spam**:確認されたスパムのみ拒否されます。
- **Spam**:システムがスパムとみなす全てのメールが拒否されます。ニュースレターなどのメールを、スパムの疑いがあるとみなして却下する場合もあるため、誤検出率が高くなる可能性があります。

SMTP トランザクション中に拒否されないメールは、以下の「*スパムフィルタ*」セクションの設定に応じて処理されます。

プロファイルモード:この設定はプロファイルごとには変更できません。メッセージが複数の受信者宛てであり、いずれかの受信者のプロファイルでスパムのスキャンが完全にオフになっている場

合、この機能は省略されます。つまり、通常のスパムスキャン設定を「*Spam*」または「*Confirmed Spam*」のいずれかにしておくことをお勧めします。

RBL（リアルタイムブラックホールリスト）

リアルタイムブラックホールリスト（RBL）とは、スパム行為に関連しているIP アドレスのリストをインターネットサイトが公開する方式です。

推奨RBLを使用:このオプションを選択すると、メール転送エージェントは外部のデータベースに対して既知のスパム送信者（いわゆる*リアルタイムブラックホールリスト*）を問い合わせます。あるサイトが、それらのリストの 1つ以上に含まれていれば、このサイトからの送信メッセージを容易に拒否することができます。このようなサービスの一部はインターネットで利用できます。この機能を使用することにより、スパムを大幅に減らすことができます。
デフォルトで、以下の RBL に対して問い合わせます。

- Commtouch IP Reputation（ctipd.org）
- cbl.abuseat.org

注 – Sophos UTMが問い合わせるRBL リストは、予告なしに変更される場合があります。Sophos は、これらのデータベースの内容を保証しません。

Sophos UTMのアンチスパム機能を強化するために、さらなるRBL サイトを追加して、アンチスパム機能を強化できます。追加するには、「*RBLゾーンの追加*」ボックスでプラスアイコンをクリックします。表示されたテキストボックスにRBL ゾーンを入力します。

設定を保存するには「*適用*」をクリックします。

スパムフィルタ

Sophos UTM Sophos UTM には、スパムの特徴があるメールをヒューリスティックにチェックする機能があります。この機能は、SMTP エンベロープ情報と、発見的テストおよび特性に関する内部データベースを使用します。このスパムフィルタオプションでは、メッセージの内容とSMTP エンベロープ情報に基づいてメッセージにスコアを付けます。スコアが高いほど、スパムの可能性が高いことを意味します。

次の 2つのオプションを使用して、ある一定のスパムスコアが付いたメッセージへの対応方法を指定することができます。これにより、ゲートウェイはスパムの可能性があるメールを別個に扱うことができるようになります。

- **Spam アクション:**ここでは、スパムの可能性があるとして分類されたメッセージに対する対策を定義できます。ここでは、誤検出、つまり、ニュースレターなどが間違ってスパムに分類さ

れ、ブラックホール化によってメールが紛失する可能性があることに注意してください。

- **Confirmed Spam アクション:**ここでは、Confirmed Spam（確実性の高いスパム）と確認されたメッセージに対するアクションを定義できます。

これら 2種類のスパムに対する処理を、さまざまな対策から選択できます。

- **オフ:**メッセージはスパムとしてマークされたり、フィルタされません。
- **警告:**メッセージはフィルタされません。受信メッセージの場合は、その代わりに、スパムフラグがメッセージヘッダに追加され、スパムマーカがメッセージの件名に追加されます。送信メッセージは、アクションなしで送信されます。
- **隔離:**メッセージはブロックされ、メールの隔離場所に保存されます。隔離されたメッセージは、ユーザポータルまたはデイリーの隔離レポートで確認できます。
- **ブラックホール:**メッセージは受信後、ただちに削除されます。送信メッセージは、意図しないメールの紛失を回避するために、ブラックホール化されることがありません。代わりに、隔離されます。

スパムマーカ:このオプションで、スパムマーカを指定できます。スパムマーカとは、スパムメッセージをすばやく簡単に識別できるように、メッセージの件名行に追加される文字列です。デフォルトでは、スパムメッセージを示すために `*SPAM*` という文字列が使用されます。

送信者ブラックリスト

受信 SMTP セッションのエンベロープ送信者は、このブラックリスト内のアドレスと照合されます。エンベロープ送信者がブラックリストに含まれている場合、メッセージはブラックホール化されます。

ブラックリストに新しいアドレスパターンを追加するには、「*ブラックリストアドレスパターン*」ボックスでプラスアイコンをクリックし、アドレス（の一部）を入力してから、「*適用*」をクリックします。ワイルドカードとしてアスタリスク（*）を使用できます（例: `*@abbeybnknational.com`）。

ヒント – エンドユーザは、ユーザポータルで独自のブラックリストおよびホワイトリストを作成できます。

表現フィルタ

表現フィルタは、SMTP プロキシを通過するメッセージに特定の表現が含まれていないか、コンテンツをスキャンし、疑いのあるメールをブロックします。表現は*Perl 互換の正規表現*で指定できます。たとえば、「online dating」などの簡単な文字列は、大文字と小文字を区別しないで解釈されます。設定を保存するには「*適用*」をクリックします。

参照 – 表現フィルタで正規表現を使用する方法の詳細は、Sophos サポートデータベースを参照してください。

高度なアンチウイルス機能

このエリアには、Sophos UTMのアンチスパム機能を強化するその他のさまざまな詳細オプションがまとめられています。

無効な HELO/RDNS 不可のリジェクト:無効なHELOエントリを送信するホストやRDNSエントリがないホストを拒否するには、このオプションを選択します。このチェックからホストを除外するには、「*除外*」タブを使用してください。

厳密なRDNSチェック:無効な RDNS レコードのホストからのメールを追加拒否するには、このオプションを選択します。RDNS レコードは、検出されたホスト名が元の IP アドレスに解決されない場合に無効になります。

グレイリスティングを使用:グレーリスト化とは、基本的に、特定の期間にわたってメールを一時的に拒否することです。一般に、グレーリスト化を使用しているメールサーバは、すべての受信メールから3種類の情報を記録します。

- 送信者のアドレス
- メッセージ送信元のホストの IP アドレス
- 受信者のアドレス
- メッセージ件名

このデータセットは、SMTP プロキシの内部データベースと照合してチェックされます。新しいデータセットが見つかった場合には、それを記述する特別なタイムスタンプとともにデータベースに記録が作成されます。このデータセットにより、当該メールが 5分間にわたって拒否されます。5分経つとプロキシがデータセットを認識します。当該メッセージが再送信されると、このメッセージは許可されます。データセットは、1週間以内に更新されなければ、1週間後に失効します。
グレイリスティングでは、ほとんどのスパムメッセージ送信者が「fire-and-forget」方式を使用している点を利用しています。これは「メールを送りつけて、うまくいかなければ忘れる」という方式です。つまり、RFC 準拠のメールサーバと違い、スパムメール送信者は、一時的な失敗が発生したメールを再送信しません。この機能では、次のことが前提となっています。つまり、一時的な失敗はメール配信に関する RFC 仕様に起因するため、正当なサーバは後でメールを再送信します。その時点で宛先にメールが受け入れられます。

BATVを使用:BATV とは、メールアドレスの正当な使用と不正な使用を区別することを目指す IETF のドラフトです。BATV は、簡単な共有鍵を追加してアドレス、時変情報、および任意のランダム

データのハッシュを符号化することにより、送信メールのエンベロープ送信者に署名を施して、メールが本当に送信者からのものであると証明する方法を提供します。これは主に、送信者自身が送信したものではないバウンスメールを拒否するために使用されます。BATV を使用することにより、受信するバウンスが本当に自分が送信したメールに由来しており、スパム送信者が偽造したアドレスからのメールではないことを確認できるようになります。戻ってきたバウンスメールのメールアドレスが BATV に従って署名されていない場合、SMTP プロキシはこのメッセージを受け付けません。BATV による署名は 7日後に失効します。メールのエンベロープの `MAIL FROM` アドレスのハッシュを符号化するために使用される鍵(あるいは *BATV シークレット*)を変更するには、「*Eメールプロテクション > SMTP > 詳細*」タブで実施します。

注 – メール転送エージェントによっては、BATV によってエンベロープ送信者アドレスが変更されたメッセージを拒否する場合があります。この場合、影響を受ける送信者、受信者、ドメインに対して除外ルールを作成する必要があります。

SPF チェックの実施:SPF(*送信者ポリシーフレームワーク*)とは、ドメインの所有者が送信メールサーバに関する情報を公開するためのフレームワークです。ドメインは公開レコードを使用して、さまざまなサービス(Web、メールなど)をこれらのサービスを実行するマシンに送信します。すべてのドメインは、そのドメインへのメールをどのマシンが受信するのかを知らせる MX レコードをメール関連のサービス用に公開しています。SPF では、ドメインからある種の「リバース MX レコード」を公開することにより、そのドメインからのメールを送信しているマシンを広く一般に伝えます。特定のドメインからメッセージを受信すると、受信者はそれらのレコードを確認して、正当な送信者からのメールであることを確認します。

参照 – 詳細は、送信者ポリシーフレームワーク の Web サイトを参照してください。

追加のアンチスパム機能として、SMTP プロキシは、任意のアドレスへのメールを受信したときに、バックエンドのメールサーバに対して受信者アドレスを暗黙でチェックしてからそのメールを受け付けます。無効な受信者アドレスへのメールは許可されません。この機能が動作するためには、使用しているバックエンドメールサーバが、SMTP ステージで不明受信者へのメールを拒否できなければなりません。原則的に、バックエンドサーバがメッセージを拒否すれば、SMTP プロキシもこのメッセージを拒否します。

ただし、受信者の確認は信頼される(許可される)ホストやリレーホストに対しては *行われません*。この理由は、ユーザエージェントによっては、SMTP トランザクションで受信者が拒否されると問題が発生する場合があるためです。一般的なシナリオ(バックエンドメールサーバが SMTP トランザクションで不明な受信者を拒否する)では、Sophos UTM バウンスが生成されるのは次の場合に限られます。

- 信頼される送信元やリレー元が、配信不能な受信者にメッセージを送信した場合。
- バックエンドメールサーバが停止しており、Sophos UTMが受信者を確認できなかった場合。

ただし、Sophos UTMは、バックエンドメールサーバからの配信不能レポート(NDR)やバウンスの送信を防止することはできません。さらにSophos UTMは、メールサーバからのスパムの可能性のあるコールアウト応答は 24時間キャッシュし、可能性のないものは2時間キャッシュします。

10.1.5 除外

「*SMTP > 除外*」タブで、アンチスパム、アンチウイルス、またはその他のセキュリティチェックから除外するホワイトリストのホスト、ネットワーク、送信者、および受信者を定義できます。

注 – メールは多数の受信者に送信される場合がありますが、Sophos UTMは SMTP プロトコルのインラインスキャニングを実装しているため、メール受信者のうち 1人でも「*受信者*」ボックスにリストされていると、メールのスキャンはすべての受信者に対してスキップされます。

除外ルールを作成するには、次の手順に従います。

1. **「*除外*」タブで、「*新規除外リスト*」をクリックします。**
   「*除外リストを作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前:この除外ルールを説明する名前を入力してください。

   実行しないチェック:スキップするセキュリティチェックを選択します。詳細は、「*Eメールプロテクション > SMTP >* アンチウイルス」および「スパム対策」を参照してください。

   送信元ホスト/ネットワークで除外:この除外ルールで定義されたセキュリティチェックをスキップする送信元ホスト/ネットワーク(メッセージが発信されたホストまたはネットワーク)を選択します。

   注 – ローカルメッセージはデフォルトでスキャンされないので、ローカルホストには除外を作成する必要はありません。

   このオプションを選択すると、「*ホスト/ネットワーク*」ボックスが開きます。「+」アイコンまたはフォルダアイコンをクリックして、ホストあるいはネットワークを追加できます。

   送信者アドレスで除外:定義したセキュリティチェックをスキップする送信者のメールアドレスを選択します。

このオプションを選択すると、「*送信者*」ボックスが開きます。完全で有効なメールアドレスを入力するか（例: `jdoe@example.com`）、またはアスタリスクをワイルドカードとして使用して特定ドメインのすべてのメールアドレスを指定できます（例: `*@example.com`）。

注 – 送信者アドレスは容易に偽造できるため、「*送信者*」オプションを使用する際は注意が必要です。

受信者アドレスで除外:定義したセキュリティチェックをスキップする受信者のメールアドレスを選択します。

このオプションを選択すると、「*受信者*」ボックスが開きます。完全で有効なメールアドレスを入力するか（例: `jdoe@example.com`）、またはアスタリスクをワイルドカードとして使用して特定ドメインのすべてのメールアドレスを指定できます（例: `*@example.com`）。

コメント（任意）:説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しい除外が「*除外*」リストに表示されます。

除外ルールを編集または削除するには、対応するボタンをクリックします。

10.1.6 リレー

SMTP プロキシはメールリレーとして使用できます。メールリレーは、特定のユーザ、ユーザグループ、あるいはホストがそれを介してローカル以外のドメインにメールをリレー（送信）できるように設定されたSMTP サーバです。

注 – このタブの一部の機能は、ベーシックガード サブスクリプションでは利用できません。

アップストリームホストリスト

アップストリームのホストは、メールをお客様の ISP あるいは外部 MX に転送するホストです。スタティックなアップストリームのホストからメールを受信する場合は、ここにホストを入力する必要があります。ホストを入力しないと、スパム保護が正常に機能しなくなります。

アップストリームホストを追加するには、「+」アイコンまたはフォルダアイコンをクリックして、「*ネットワーク*」オブジェクトリストからドラッグ＆ドロップします。アップストリームホストのみを許可する場合は、「*アップストリーム/リレーホストのみ許可*」チェックボックスにチェックを入れます。これにより、SMTP アクセスは、定義されたアップストリームホストに制限されます。アップストリームホストは、リレー特権の取得を認証できます。設定を保存するには「*適用*」をクリックします。

認証リレー

SMTP クライアントは、リレー特権の取得を認証できます。「*認証によるリレーの許可*」チェックボックスにチェックを入れて、この機能を使用できるようにするユーザおよびユーザグループを指定します。設定を保存するには「*適用*」をクリックします。

注 –「*アップストリーム/リレーホストのみ許可*」チェックボックスにチェックが入っている場合、*認証リレー*は送信ホストがアップストリーム/リレーホストとして設定されている場合にのみ機能します。

ホストベースリレー

メールリレーも、ホストベースに対応できます。お使いのローカルメールサーバあるいはメールクライアントが SMTP プロキシをメールリレーとして使用する必要がある場合は、リレーを介してメールを送信できるようにするネットワークやホストを「*許可ホスト/ネットワーク*」ボックスに追加する必要があります。リストされたネットワークやホストは、どのアドレスにもメッセージを送信できます。

警告 –「*許可ホスト/ネットワーク*」ボックスでは、絶対に「すべて」を選択しないでください。これを選択すると、オープンリレーになり、インターネット上の誰もが SMTP プロキシ経由でメッセージを送信できるようになります。スパマはこれをすぐに見つけ、大量のメールトラフィックを送信します。最悪の場合は、お客様がサードパーティのスパマブラックリストに載ることになってしまいます。ほとんどの設定では、お客様のネットワークのメールサーバだけを、メールのリレーを許可される唯一のホストとすべきです。

設定を保存するには「*適用*」をクリックします。

ホスト/ネットワークのブラックリスト

ここで、SMTP プロキシでブロックするホストおよびネットワークを定義できます。設定を保存するには「*適用*」をクリックします。

リレー(送信)メッセージのコンテンツをスキャン

このオプションを有効にすると、認証されたリレーあるいはホストベースのリレーで送信されるメッセージについて、悪意あるコンテンツの有無がスキャンされます。送信メールが大量にある場合、このオプションをオフにすると、パフォーマンスが向上します。設定を保存するには「*適用*」をクリックします。

送信メッセージには、グローバルなアンチウイルスおよびアンチスパム設定も適用されます。ただし、これらの設定を問わず、感染メッセージやスパムメッセージはブラックホール化ではなく常に隔離されます。これにより、意図しないメールの紛失が回避されます。

10.1.7 詳細

「*SMTP > 詳細*」タブでは、スマートホストの設定や透過モードスキップリストなどの SMTP プロキシの追加セキュリティオプションを設定できます。

親プロキシ

親プロキシは、多くの場合、政府承認のプロキシサーバを通してインターネットアクセスをルーティングする必要のある国などで必要とされます。親プロキシの使用がセキュリティポリシーで求められている場合、ここでホスト定義とポートを選択して親プロキシを設定できます。

親プロキシを使用:親プロキシの使用を有効にするには、チェックボックスにチェックを入れます。プロキシのホスト名とポートを入力します。

プロキシ認証が必要:親プロキシで認証が必要な場合、ここでユーザ名とパスワードを入力します。

透過モード

SMTP の透過モードを有効にするには、チェックボックスにチェックを入れ、「*適用*」をクリックします。

「*透過モード時にスキップするホスト/ネット*」ボックスにリストされているホストとネットワークは、SMTP トラフィックの透過的インターセプションの対象とはなりません。ただし、これらのホストおよびネットワークで SMTP トラフィックを許可するには、*「リスト内のホスト/ネットワークの SMTP トラフィックを許可」*チェックボックスにチェックを入れます。このチェックボックスにチェックを入れない場合は、ここでリストされているホストとネットワークに特定のファイアウォールルールを定義する必要があります。

TLS設定

TLS証明書ドロップダウンリストから証明書を選択します。この証明書は、TLS 暗号化についてそれをサポートしているすべてのリモートホストとネゴシエートするために使用されます。証明書は、「*サイト間 VPN > 証明書管理 > 証明書*」タブで作成またはアップロードできます。

TLS ネゴシエーション必須のホスト/ネット:ここに、メール通信の TLS 暗号化が常に必要なホストまたはネットを追加します。これにより、UTMは、これらのホスト/ネットで何らかの理由で TLS 暗号化を使用できない場合に、メールを抑制します。つまり、TLS が使用可能になるまで、メッセージは

メールキューに保留されます。一定の期間にわたって TLS を使用できない場合は、送信の試行が停止され、メールを送信できなかったという通知がユーザに送信されます。

TLS ネゴシエーション必須の送信ドメイン:特定のドメインに対して受信メールの TLS 暗号化を強制するには、ここにドメインを入力します。これらのドメインから TLS なしで送信されたメールは、即時に拒否されます。

TLS ネゴシエーションをスキップするホスト/ネット:特定のホストやネットワークで TLS 暗号化に関する問題が発生した場合は、それをボックスに入力し、適切な TLS 証明書をドロップダウンメニューから選択します。それによって、UTMは、このホストまたはネットワークに対するTLSネゴシエーションをスキップします。設定を保存するには「*適用*」をクリックします。

DomainKeys Identified Mail (DKIM)

DKIM は発信メッセージに暗号によって署名する方法です。DKIM 署名を使用するには、RSA 鍵と対応する鍵セレクタを各フィールドに入力し、メールに署名するドメインを「*DKIM ドメイン*」ボックスに追加します。設定を保存するには「*適用*」をクリックします。

機密性表明フッタ

各送信メールについて、メールに機密情報や部外秘の情報が含まれていることなどをユーザに知らせる、機密フッタを追加してカスタマイズできます。なお、機密フッタは、返信メールの場合（*In-Reply-To*ヘッダを持つもの）、またはメールのコンテンツタイプを判定できない場合は、メールに追加されません。

注 –メールクライアント（例: Microsoft Outlook または Mozilla Thunderbird）が署名済みまたは暗号化済みのメッセージにフッタを追加すると、署名が破壊されて無効になります。デジタル署名をクライアント側で作成する場合は、アンチウイルスチェックフッタオプションを無効にしてください。ただし、メール通信のプライバシーや認証を保ちながら、一般的なウイルス対策チェックフッタを使用する場合は、Sophos UTM の組み込みメール暗号化機能の使用を考慮してください。ゲートウェイ上でのメール暗号化では、デジタル署名を作成する前にフッタがメッセージに付加されるため、署名が損なわれることはありません。

詳細設定

ここで、SMTP ホスト名やポストマスタアドレスなどを設定できます。

SMTP ホスト名:SMTP ホスト名を設定すると、プロキシは、HELO および SMTP バナーメッセージで指定された名前を使用します。デフォルトでは、通常システムのホスト名が選択されています。

Postmasterアドレス:送信されたメッセージの転送先となるUTMのポストマスタのメールアドレスを`postmaster@[192.168.16.8]`の形で指定します。この場合、IP リテラルアドレスが、UTMの IP アドレスの1つになります。そのようなメッセージを受け入れることが RFC 要件となっています。

BATV シークレット:ここで、SMTP プロキシが使用する、自動的に生成された BATV シークレットを変更できます。BATV シークレットはメールのエンベロープの `MailFrom` アドレスへの署名に使用される共有鍵で、無効なバウンスアドレスの検出を可能にします。複数の MX をドメインに使用している場合は、BATV シークレットをすべてのシステムで同じものに変更できます。

最大メッセージサイズ:プロキシが受け付ける最大メッセージサイズ。この設定は送受信両方のメールに適用されます。バックエンドサーバにメッセージサイズの制限がある場合は、ここではその制限値以下に設定する必要があります。

最大コネクション数:プロキシが許可する最大同時接続数。デフォルトは 20 です。

最大コネクション数/ホスト:プロキシが許可するホスト当たりの最大接続数。デフォルトは 10 す。

最大メール数/コネクション:プロキシが許可するコネクション当たりの最大メール数。デフォルトは 1000 です。

最大受信者数/メール:プロキシが許可するメール当たりの最大受信者数。デフォルトは 500 です。

フッタモード:ここでメールへのフッタの追加方法を定義できます。「*MIME パート*」を指定すると、追加の MIME パートとしてフッタを追加します。既存のパートエンコーディングは変更されないので、国語の文字が保持されます。別の方式である「*インライン*」では、フッタがメール本体から区切り記号 `--` で分離されます。このモードでは、フッタで Unicode (UTF-8) 変換を使用するかどうかを選択できます。Unicode 変換を行うと、フッタで国語の文字を保持するようにメッセージがアップグレードされます。

スマートホストの設定

スマートホストはメールリレーサーバの一種で、SMTP サーバが受信者のサーバに直接メールをルーティングするのではなく、アップストリームのメールサーバにルーティングできるようにします。多くの場合このスマートホストは、送信者がスマートホストを通してメールを送信する権限を持つことを確認するために、送信者の認証を必要とします。

スマートホストを使用:メールの送信にスマートホストを使用する場合は、このチェックボックスにチェックを入れます。このオプションを選択すると、プロキシ自体がメールを配信することはなくなり、すべてをスマートホストに送信するようになります。

- **スマートホスト:**スマートホストオブジェクトを選択または追加します。
- **スマートホストポート:**スマートホスト接続のデフォルトポートは25です。必要に応じて、ポートを変更できます。

- **スマートホスト認証が必要:**スマートホストが認証を必要とする場合は、チェックボックスにチェックを入れます。「*プレーン*」と「*ログイン*」認証タイプの両方がサポートされています。それぞれのフィールドにユーザ名とパスワードを入力します。

10.2 SMTP プロファイル

Sophos UTMの SMTP プロキシで、別の SMTP プロファイルを作成し、それを異なるドメインに関連付けることができます。このようにして、「*Eメールプロテクション > SMTP*」で設定されたデフォルトのプロファイル以外のプロファイルを使用する特定のドメインを指定できます。機能の順序はタブによって構造化され、SMTP トランザクション時に各ステップが互いにどのように処理されるかを決定します。

SMTP プロファイルを作成するには、以下の手順に従います。

1. **SMTP プロファイルモードを有効にします。**
「*Eメールプロテクション > SMTP > グローバル*」タブで、「*プロファイルモード*」を選択して「*適用*」をクリックします。

   「*Eメールプロテクション > SMTP プロファイル (SMTP Profiles)*」メニューの SMTP プロファイル作成が有効になります。

2. **「*SMTP プロファイル*」タブで、「*新規プロファイル*」をクリックします。**
ダイアログボックスが開きます。

3. **プロファイルを説明する名前を入力してください。**

4. **1つ以上のドメインを追加します。**
1つ以上のドメインを「*ドメイン*」ボックスに追加します。

   このプロファイルの設定が、それらのドメインに適用されます。

5. **次の設定を行います。**
使用する機能にのみ設定します。以下の各機能に対して、ここで定義する個々の設定を使用するか、または「*Eメールプロテクション > SMTP*」で定義するグローバル設定を使用するかを決定できます。デフォルトでは、グローバル設定オプションが選択されています。各機能の個々の設定について以下に説明します。

   注 – ここで設定されたドメイン名が送信者アドレスに含まれる暗号化されたメールは、Sophos UTMのメール暗号化/復号化エンジンを使用しても復号化できません。したがって、外部メールドメインのプロファイルは含めないようにしてください。

ここで定義できるすべての設定は、「*Eメールプロテクション > SMTP*」でもグローバルに設定できます。したがって、ここでは、設定の一覧とグローバル設定との相違点のみを、対応するグローバル設定へのクロスリファレンスとともに示します。設定の詳細は、グローバル設定でご覧ください。

以下の設定を行うことができます。

- **ルーティング:**「*ルーティング*」タブで、SMTP プロキシのドメインとルーティングターゲットを設定し、受信者の確認方法を定義します。
  - スタティックホストリスト (Static Host List)
  - DNS ホスト名 (DNS Hostname)
  - MX レコード (MX Records)

  詳細は、「*Eメールプロテクション > SMTP > ルーティング*」を参照してください。

- **受信者検証**
  受信者検証:ここでメール受信者を確認するかどうかと確認方法を指定できます。
  - **コールアウト使用:**受信者検証の要求がサーバに送信されます。
  - **Active Directory使用:**受信者検証の要求が Active Directory サーバに送信されます。Active Directory を使用するには、「*定義とユーザ > 認証サーバ > サーバ*」で指定された Active Directory サーバを備えていることが必要です。ベース DN を「*代替ベース DN*」フィールドに入力します。

    注 – Active Directory 受信者検証を使用すると、サーバが応答しない場合にメッセージがバウンスされる場合があります。

  - **オフ:**受信者検証は完全にオフにできますが、推奨されません。なぜなら、オフにすると、スパムトラフィックが増大して、辞書攻撃の危険性が高まるからです。この結果、隔離場所が迷惑メールで溢れてしまうことになります。

  詳細は、「*Eメールプロテクション > SMTP > ルーティング*」を参照してください。

- **Sophos UTM RBL:**ここでスパムにリンクした IP アドレスをブロックできます。
  - 推奨された RBL を使用 (Use Recommended RBLs)
  - ダイヤルアップ/レジデンシャルホストのブロック

  詳細は、「*Eメールプロテクション > SMTP > スパム対策*」を参照してください。

- **追加RBL:**Sophos UTMのアンチスパム機能を強化するために、さらなる RBL サイトを追加できます。詳細は、「*メールプロテクション > SMTP > スパム対策*」を参照してくだ

さい。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。

- **BATV/RDNS/HELO/SPF/Greylisting:**このエリアには、Sophos UTMのアンチスパム機能を強化するその他のさまざまな詳細オプションがまとめられています。
  - 無効な HELO/RDNS なしのリジェクト
  - グレイリスティングを使用
  - BATV を使用
  - SPF チェックを実施

  詳細は、「*Eメールプロテクション > SMTP > スパム対策*」を参照してください。

- **アンチウイルススキャン:**悪意あるコンテンツを含むメッセージの処理方法を設定できます。次の作業を実行できます。
  - オフ
  - 隔離
  - ブラックホール

  以下のアンチウイルススキャンオプションから選択できます。

  - **シングルスキャン:**デフォルト設定。「スキャン設定」タブに定義されたエンジンを使用して最高レベルのパフォーマンスを実現します。
  - **デュアルスキャン:**各トラフィックに対し、異なるウイルススキャナを使用してスキャンを 2回行うことにより、検出率を最大限に高めます。ベーシックガードサブスクリプションではデュアルスキャンは利用できません。

  スキャンできないコンテンツ、暗号化されたコンテンツの隔離:このオプションを選択して、コンテンツをスキャンできなかったメールを隔離します。スキャンできないコンテンツは、暗号化されたもの、破損したアーカイブ、またはサイズが大きすぎるコンテンツの他、スキャナの不具合などの技術的な問題による場合があります。

  詳細は、「*Eメールプロテクション > SMTP > アンチウイルス*」を参照してください。

- **アンチスパムスキャン:**ここで迷惑な宣伝メールの取り扱いを決めます。スパムおよびスパムと確認されたメールに対して以下の対策を選択できます。
  - オフ
  - 警告
  - 隔離
  - ブラックホール

詳細は、「*Eメールプロテクション > SMTP > スパム対策*」を参照してください。

- **送信者ブラックリスト:**受信 SMTP セッションのエンベロープ送信者は、このブラックリスト内のアドレスと照合されます。エンベロープ送信者がブラックリストに含まれている場合、メッセージはブラックホール化されます。詳細は、「*Eメールプロテクション > SMTP > スパム対策*」を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。
- **MIME オーディオ/ビデオ/実行形式ブロック:**MIME タイプのフィルタは MIME タイプのメールコンテンツを読みます。どのタイプのコンテンツを隔離するかを選択できます。
  - 音声コンテンツ
  - 動画コンテンツ
  - 実行可能ファイルコンテンツ

  詳細は、「*Eメールプロテクション > SMTP > アンチウイルス*」を参照してください。
- **MIMEタイプブラックリスト:**ここで、その他の MIME タイプを隔離場所（検疫）に追加できます。詳細は、「*Eメールプロテクション > SMTP > アンチウイルス*」を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。
- **MIMEタイプホワイトリスト:**ここで、隔離しない MIME タイプを追加できます。詳細は、「*Eメールプロテクション > SMTP > アンチウイルス*」を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。
- **ブロック対象ファイル拡張子:***ファイル拡張子フィルタ*を使用して、ファイル拡張子に基づいて、特定のファイルタイプ（例: 実行可能ファイル）を含むメールを（警告付きで）隔離できます。詳細は、「*Eメールプロテクション > SMTP > アンチウイルス*」を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。
- **ブロック対象表現:**表現フィルタは、SMTP プロキシを通過するメッセージに特定の表現が含まれていないか、コンテンツをスキャンし、疑いのあるメールをブロックします。詳細は、「*Eメールプロテクション > SMTP > スパム対策*」を参照してください。3番目のオプションとして、ここで個別の設定にグローバル設定を追加できます。
- **機密性表明フッタ:**各送信メールについて、メールに機密情報や部外秘の情報が含まれていることなどをユーザに知らせる、機密フッタを追加してカスタマイズできます。なお、機密フッタは、返信メールの場合（*In-Reply-To*ヘッダを持つもの）、またはメールのコンテンツタイプを判定できない場合は、メールに追加されません。送信者ドメインに応じて、フッタが追加されます。フッタを使用するには、チェックボックスにチェックを入れ、フッタのテキストを入力して「*適用*」をクリックします。

6. **「*適用*」をクリックします。**
   設定が保存されます。新しいプロファイルが「*SMTP プロファイル*」リストに表示されます。

注 – トピックに「*グローバル設定の使用*」を選択して、「*適用*」をクリックすると、機能のアイコンがグローバル設定のアイコンに変わります。これにより、どの機能に対してグローバル設定または個々の設定が適用されているかが簡単にわかります。

プロファイルの無効化、名前変更、または削除を行う場合は、プロファイルドロップダウンリスト下にある上段の該当するボタンをクリックします。

10.3 POP3

「*Eメールプロテクション > POP3*」メニューでは、受信メールの POP3 プロキシを設定できます。*Post Office Protocol 3* (POP3) はアプリケーション層インターネット標準プロトコルで、リモートメールサーバからのメールの取り出しを可能にします。POP3 プロキシは透過的に機能します。つまりポート `110` または `995` (TLS による暗号化) で内部ネットワークから受信するすべての POP3 要求は、クライアントには認識されずにプロキシを通して傍受され、リダイレクトされます。このモードのメリットは、その他の管理やクライアント側の設定が必要ないということです。

注 – 場合によっては、メールクライアントの設定でサーバタイムアウト設定を長くすることが必要です。通常のデフォルトである約 1分以内の設定では、特に大きなメールをフェッチするときには短すぎます。

POP3 プロトコルには、どのメールがすでに取り出されたかをサーバ側で追跡する機能はありません。一般的には、メールクライアントがメールを取り出した後、サーバ上でそれを削除します。ただし、クライアントがメールを削除しないように設定されている場合、サーバ側の削除は行われず、どのメールがすでにフェッチされたかをクライアントが追跡します。

10.3.1 グローバル

「*Eメールプロテクション > POP3 > グローバル*」タブでは、POP3 プロキシの基本設定を構成できます。

POP3 プロキシを設定するには、以下の手順に従います。

1. **POP3 プロキシを有効にします。**
   トグルスイッチをクリックします。

トグルスイッチがアンバー色になり、「*POP3 設定*」エリアが編集可能になります。

2. **許可するネットワークを選択します。**
   プロキシ POP3トラフィックに許可するネットワークを選択します。通常、これは内部ネットワークです。
3. **「*適用*」をクリックします。**
   設定が保存されます。

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

ライブログ

「*POP 3 ライブログ*」は、POP3プロキシのアクティビティをログに記録し、すべての受信メールを表示します。ボタンをクリックして、新しいウィンドウでライブログを開きます。

10.3.2 ウイルス対策

「*アンチウイルス*」タブには、ウイルス、ワーム、その他のマルウェアなどの有害で危険なコンテンツを含むメールに対するさまざまな対策が含まれています。

アンチウイルススキャン

このオプションでは、ウイルス、トロイの木馬、疑わしいファイルタイプなどの不要なコンテンツがないかどうか、メールをスキャンします。悪意のあるコンテンツを含むメッセージはブロックされて、メールの隔離場所に保存されます。ユーザは、Sophosユーザポータル またはデイリーの隔離レポートで、隔離されたメッセージを確認してリリースできます。ただし、悪意のあるコンテンツを含むメッセージは、メールマネージャで管理者のみが隔離からリリースできます。

Sophos UTM は、最高のセキュリティを実現するさまざまなアンチウイルスエンジンを備えています。

- **シングルスキャン:**デフォルト設定。「*スキャン設定*」タブに定義されたエンジンを使用して最高レベルのパフォーマンスを実現します。
- **デュアルスキャン:**各トラフィックに対し、異なるウイルススキャナを使用してスキャンを 2回行うことにより、検出率を最大限に高めます。ベーシックガードサブスクリプションではデュアルスキャンは利用できません。

スキャンできないコンテンツ、暗号化されたコンテンツの隔離:このオプションを選択して、コンテンツをスキャンできなかったメールを隔離します。スキャンできないコンテンツは、暗号化されたもの、破損したアーカイブ、またはサイズが大きすぎるコンテンツの他、スキャナの不具合などの技術的な問題による場合があります。

最大スキャンサイズ:アンチウイルスエンジンでスキャンする最大ファイルサイズを指定します。このサイズを超えるファイルはスキャン対象外となります。

設定を保存するには「*適用*」をクリックします。

ファイル拡張子フィルタ

この機能は、ファイル拡張子に基づいて特定タイプのファイル(実行可能ファイルなど)を含むメールを(警告付きで)フィルタリングし、隔離します。ファイル拡張子を追加するには、「*ブロック対象ファイル拡張子*」ボックスの「+」アイコンをクリックし、スキャンするファイル拡張子(例: `exe` または `jar`(区切り文字のドットなし))を入力します。設定を保存するには「*適用*」をクリックします。

ヒント – 禁止されたファイル拡張子に対してアーカイブを検索することはできません。アーカイブに含まれるマルウェアからネットワークを保護するには、該当するアーカイブのファイル拡張子をブロックすることを考慮してください。

10.3.3 スパム対策

Sophos UTM Sophos UTM を設定して、未承諾のスパムメールを検出したり、既知の(または疑わしい)スパム発信者からのスパム送信を識別することができます。「*スパム対策*」タブにある設定オプションを使用して、POP3 のセキュリティ機能を設定し、未承諾の宣伝用メールなどからネットワークを保護します。

スパムフィルタ

Sophos UTM Sophos UTM には、スパムの特徴がある受信メールをヒューリスティックにチェックする機能があります。この機能は、SMTP エンベロープ情報と、発見的テストおよび特性に関する内部データベースを使用します。このスパムフィルタオプションでは、メッセージの内容と SMTP エンベロープ情報に基づいてメッセージにスコアを付けます。スコアが高いほど、スパムの可能性が高いことを意味します。

次の 2つのオプションを使用して、ある一定のスパムスコアが付いたメッセージへの対応方法を指定することができます。これにより、ゲートウェイはスパムの可能性があるメールを別個に扱うことができるようになります。

- **Spamアクション:**ここでは、スパムの可能性があるとして分類されたメッセージに対する対策を定義できます。
- **Confirmed Spamアクション:**ここでは、Confirmed Spam(確実性の高いスパム)と確認されたメッセージに対するアクションを定義できます。

これら 2種類のスパムに対する処理を、さまざまな対策から選択できます。

- **オフ:**メッセージはスパムとしてマークされたり、フィルタされません。
- **警告:**メッセージはフィルタされません。その代わりに、スパムフラグがメッセージヘッダに追加され、スパムマーカがメッセージの件名に追加されます。
- **隔離:**メッセージはブロックされ、メールの隔離場所に保存されます。隔離されたメッセージは、ユーザポータルまたはデイリーの隔離レポートで確認できます。

スパムマーカ:このオプションで、スパムマーカを指定できます。スパムマーカとは、スパムメッセージをすばやく簡単に識別できるように、メッセージの件名行に追加される文字列です。デフォルトでは、スパムメッセージを示すために `*SPAM*` という文字列が使用されます。

表現フィルタ

表現フィルタは、特定の表現を探してメッセージの件名や本文をスキャンします。ここにリストされた表現を含むメールはブロックされます。ただし、*「Eメールプロテクション」>「POP3」>「詳細」*タブでプリフェッチオプションが有効になっている場合は、メールは隔離場所に送られます。表現は *Perl 互換の正規表現*で指定できます。たとえば、「online dating」などの簡単な文字列は、大文字と小文字を区別しないで解釈されます。

参照 – 表現フィルタで正規表現を使用する方法の詳細は、Sophos サポートデータベースを参照してください。

設定を保存するには「*適用*」をクリックします。

送信者ブラックリスト

受信するPOP3セッションのエンベロープの送信者が、このブラックリストのアドレスと照合されます。エンベロープの送信者がブラックリストにある場合、メッセージは隔離され、件名行に *Other* とマークされます。

ブラックリストに新しいアドレスパターンを追加するには、「*ブラックリストアドレスパターン*」ボックスでプラスアイコンをクリックし、アドレス（の一部）を入力してから、「*適用*」をクリックします。ワイルドカードとしてアスタリスク(*)を使用できます（例: `*@abbeybnknational.com`）。

ヒント – エンドユーザは、ユーザポータルで独自のブラックリストおよびホワイトリストを作成できます。

10.3.4 除外

「*POP3 > 除外*」タブで、さまざまなセキュリティ機能から除外するクライアントホスト/ネットワークや送信者アドレスを定義できます。

除外ルールを作成するには、次の手順に従います。

1. **「*除外*」タブで、「*新規除外リスト*」をクリックします。**
   「*除外リストを作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前:この除外ルールを説明する名前を入力してください。

   スキップするチェック:スキップするセキュリティチェックを選択します。詳細は、*「Eメールプロテクション」>「SMTP」>「アンチウイルス」*および「スパム対策」を参照してください。

   クライアントホスト/ネットワークで除外:セキュリティチェックをスキップする送信元ホスト/ネットワーク(メッセージを発信したホストまたはネットワーク)を選択します。

   注 – ローカルメッセージはデフォルトでスキャンされないので、ローカルホストには除外を作成する必要はありません。

   このオプションを選択すると、「*クライアントホスト/ネットワーク*」ダイアログボックスが開きます。「+」記号またはフォルダ記号をクリックして、ホストあるいはネットワークを追加できます。

   送信者アドレスで除外:定義したセキュリティチェックをスキップする送信者のメールアドレスを選択します。
   このオプションを選択すると、「*送信者*」ボックスが開きます。完全で有効なメールアドレスを入力するか(例: `jdoe@example.com`)、またはアスタリスクをワイルドカードとして使用して特定ドメインのすべてのメールアドレスを指定できます(例: `*@example.com`)。

   注 – 送信者アドレスは容易に偽造できるため、「*送信者*」オプションを使用する際は注意が必要です。

   コメント(任意):説明などの情報を追加します。
3. **「*保存*」をクリックします。**
   新しい除外が「*除外*」リストに表示されます。

除外ルールを編集または削除するには、対応するボタンをクリックします。

10.3.5 詳細

「*POP3 > 詳細*」タブで、POP3プロキシの透過モードをスキップできるホストとネットワークを指定できます。さらに、このタブには、POP3プロキシのプリフェッチオプションが含まれています。プリ

フェッチオプションにより、POP3 サーバからメッセージをプリフェッチ（事前取得）してデータベースに保存できます。

透過モードスキップリスト

「*透過モード時にスキップするホスト/ネット*」ボックスにリストされているホストとネットワークは、POP3 トラフィックの透過的インターセプションの対象とはなりません。ただし、これらのホストおよびネットワークで POP3 トラフィックを許可するには、「*リスト内のホスト/ネットワークの POP3 トラフィックを許可*」チェックボックスにチェックを入れます。このチェックボックスにチェックを入れない場合は、ここでリストされているホストとネットワークに特定のファイアウォールルールを定義する必要があります。

POP3 サーバとプリフェッチ設定

ネットワークまたはエンドユーザが使用する POP3 サーバをここに 1つ以上入力して、プロキシが認識するようにします。さらに、プリフェッチをオンにできます。

POP3 サーバを定義するには、次の手順に従います。

1. **POP3 サーバの DNS 名を追加します。**
   「*POP3 サーバ*」ボックスで、「+」アイコンをクリックします。「*サーバの追加*」ダイアログウィンドウで、DNS 名を入力し、「*保存*」をクリックします。

   入力した DNS 名にサフィックス「*Servers*」が追加された新しいエントリがボックスに表示されます。UTM は指定した DNS 名の DNS グループを自動的に作成し、新しい POP3 サーバのエントリに関連付けます。

2. **POP3 サーバの属性を指定します。**
   「*POP3 サーバ*」ボックスで、POP3 サーバの編集アイコンをクリックします。「*サーバを編集*」ダイアログボックスが開きます。次の設定を行います。

   名前:必要に応じて POP3 サーバ名を変更します。

   ホスト:ボックスには、上記で指定した DNS 名の DNS グループが自動的に入ります。追加のホストまたは DNS グループを追加または選択します。同じ POP3 アカウントを持つホストまたは DNS グループのみを追加します。

   TLS 証明書:ドロップダウンリストから証明書を選択します。この証明書は、TLS 暗号化についてそれをサポートしているすべてのリモートホストとネゴシエートするために使用されます。証明書は、「*サイト間 VPN > 証明書管理 > 証明書*」タブで作成またはアップロードできます。

注 – ここで定義しないPOP3サーバ、またはTLS証明書を持たないPOP3サーバについては、デフォルトのTLS証明書を「*TLS設定*」セクションで選択できます。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   POP3サーバが定義されます。

POP3サーバを指定しない場合にプロキシがメールを確認すると、プロキシは同じ接続でそのメールの代わりに、メールを隔離したことを受信者に通知するメッセージをただちに送ります。隔離されたメールは「*メールマネージャ*」で表示できますが、サーバやアカウントに関連付けられていないため、後から接続してリリースする(取り出して再配信する)ことはできません。一般的には、隔離されたメールのリリースは、プリフェッチされたメッセージのみで有効です。

以下の2つのシナリオがあります。

- POP3サーバを指定してプリフェッチを無効にした場合、プロキシは、隔離されたメールがどのサーバ/アカウントに属するかを追跡します。したがって、隔離されたメールは、クライアントがメールボックスを次回ポーリングしたときにリリースできます。これが機能するには、プロキシは、どのIPアドレスがどのサーバに属するかを(お客様がメールクライアントで入力したFQDNによって)確実に特定する必要があります。
- POP3サーバを指定してプリフェッチを有効にした場合、POP3プロキシは新しいメッセージがないかどうかPOP3サーバを定期的に確認します。新しいメッセージが届いている場合、それはPOP3プロキシにコピーされ、スキャンされて、UTMのデータベースに保存されます。メッセージはPOP3サーバに留まります。クライアントは新しいメッセージをフェッチする(取り出す)とき、POP3プロキシと通信して、このデータベースからメッセージを取り出します。

プリフェッチをサポートしているPOP3プロキシには、以下のようなさまざまなメリットがあります。

- クライアントとプロキシ(またはその逆)のタイムアウトの問題はありません。
- メールを事前にスキャンするため、メッセージははるかに迅速に配信されます。
- ブロックされたメッセージはユーザポータルからリリースでき、次のフェッチに含まれます。

メッセージが悪意のコンテンツを含んでいたためにブロックされた場合、またはスパムと特定されたためにブロックされた場合は、クライアントには配信されません。それらのメッセージは隔離されます。隔離されたメッセージはユーザポータルの「*メールマネージャ*」セクションに保存され、そこで削除またはリリースされます。

プリフェッチモードを使用:プリフェッチモードを有効にするには、このチェックボックスを選択して、1つ以上のPOP3サーバを「*POP3サーバ*」ボックスに追加します。

プリフェッチ間隔:POP3プロキシがPOP3サーバに接触してメッセージをプリフェッチする時間間隔を選択します。

注 – メールクライアントがPOP3サーバへの接続を許可される間隔は、サーバごとに異なります。したがって、プリフェッチ間隔は、POP3サーバで許可されている間隔より短く設定しないようにしてください。この理由は、POP3サーバへのアクセスがブロックされると、POP3メッセージのダウンロードは失敗に終わるからです。
また、複数のメールクライアントが同じPOP3アカウントをクエリする場合があることにも注意してください。POP3サーバからメッセージがフェッチされると、次回サーバにアクセスできるようになるまでタイマーが再始動します。このためにPOP3プロキシがPOP3サーバに4回連続してアクセスできないと(デフォルトでは15分ごとにアクセスを試行します)、アカウントのパスワードがプロキシのメールデータベースから削除され、メールクライアントがPOP3サーバにパスワードを再度送ってログインしない限り、メールはフェッチされなくなります。

隔離メールをサーバから削除:このオプションを選択すると、隔離されたメッセージはPOP3サーバから即座に削除されます。これは、ユーザがUTM経由ではなく、たとえば、POP3サーバのWebポータル経由でPOP3サーバに接続した場合に、スパムやウイルスメッセージの受信を防ぐのに役立ちます。

メッセージを取り出した後にサーバからメッセージを削除するようにメールクライアントが設定されている場合、この情報はデータベースにも保存されます。プロキシは、次回このPOP3アカウントのメッセージをプリフェッチするときに、サーバからそれらのメッセージを削除します。これは、クライアントがSophos UTMからメッセージをフェッチせず、かつ、削除コマンドが設定されていない限り、メッセージはPOP3サーバから削除されないことを意味します。したがって、それらはまだ、たとえばメールプロバイダーのWebポータルで読むことができます。
以下の場合、隔離されたメッセージはPOP3サーバから削除されます。

- メッセージをメールマネージャで手動で削除した場合。
- ユーザがユーザポータルでメッセージを手動で削除した場合。
- メッセージが(隔離レポートまたはユーザポータルのいずれかを介して)リリースされ、配信時にメッセージを削除するようにユーザのメールクライアントが設定されている場合。
- 通知メッセージが削除された場合。
- 保存期間が過ぎた場合(メールマネージャの章の「設定」のセクションを参照してください)。

ただし、プリフェッチモードでは、隔離されたスパムメッセージは、クライアントコマンドではPOP3サーバから直接削除できません。

注 – プリフェッチ機能が正常に機能するためには、メールクライアントは少なくとも 1回は POP3 サーバに接続する必要があります。これは、このユーザのために POP3 メッセージをフェッチするには、Sophos UTMは、POP3 サーバ名、ユーザ名、およびユーザのパスワードをデータベースに保存する必要があるからです。ただし、これは、Sophos ユーザポータルで POP3 アカウントの資格情報を設定しても、機能*しません*。プリフェッチされたメッセージをこのユーザのポータルと毎日の隔離レポートに表示するには、ユーザポータルで POP3 アカウント資格情報が必要です。

fetchmail ユーザへの注記:セキュリティ上の理由から、メールサーバからのメールのダウンロードに `TOP` メソッドはサポートされていません。したがって、`TOP` によって受信したメッセージはスキャンできません。ただし、`fetchall` オプション(コマンドラインの `-a`)を指定するとスキャンできます。詳細は、fetchmail のマニュアルの「RETR または TOP」を参照してください。

優先文字コード

このセクションでは、メールヘッダは、何らかの理由でUTMによって変更された(例:BATV)メールヘッダで今後使用する UTF-8 以外の文字コードを選択できます。この機能は、UTF-8 を理解しないメールクライアントをユーザが使用している場合に便利です。一般に、メールヘッダのデフォルトの文字セットはすべての地域で問題なく機能します。したがって、この設定を変更するのは、これが絶対に必要であると確信している場合の*み*にしてください。不明な場合は、デフォルトの *UTF-8* にしておいてください。

TLS 設定

TLS 証明書ドロップダウンリストから証明書を選択します。この証明書は、TLS に対応しており、上記の「*POP3 サーバ*」ボックスに表示されていない POP3 サーバや、一致する TLS 証明書のない POP3 サーバにアクセスを試みるすべての POP3 クライアントで、TLS 暗号化のために使用されます。選択した証明書は POP3 クライアントに提供されます。通常、POP3 クライアントは、POP3 サーバから提供された TLS 証明書が、設定*済み* POP3 サーバの名前に一致しているか確認します。このため、多くの場合 POP3 クライアントは、証明書のホスト名が設定*済み* POP3 サーバ名に一致しないとして、警告を表示します。ただし、ユーザはこの警告を無視して接続することができます。この警告を回避するには、使用したすべての POP3 サーバを上記の「*POP3 サーバ*」ボックスに追加し、各サーバに一致する TLS 証明書を指定してください。

ここで証明書を一つも設定しないと、POP3 クライアントが TLS を介して「*POP3 サーバ*」ボックスのリストにない、または、一致する TLS 証明書を持たない POP3 サーバにアクセスしようとした場合、接続は確立されません。

ヒント–証明書は、「*サイト間 VPN > 証明書管理 > 証明書*」タブで作成またはアップロードできます。

10.4 暗号化

メールが個人的な目的やビジネス目的で使用する主な電子通信手段となって以来、プライバシーや認証に関する懸念が高まっています。メールは平文形式で伝送されますが、これを一般的に言うと、ハガキと同じようにすべての人が読めるということです。さらに、身元を偽るのが容易であるため、送信者が本当に本人であるかどうかを受信者が見分けられることは重要です。

通常、これらの問題はメールの暗号化とデジタル署名で解決できます。これにより、メールメッセージは電子的に署名され、暗号によって符号化されます。この結果、メールを開いてコンテンツを閲覧できるのはメッセージ受信者のみとなり(プライバシー)、送信者の身元が確認されるようになります(認証)。つまり、このプロセスでは「ハガキの電子版」を送付するという考えが否定され、書留郵便や配達証明郵便に近いプロセスとなります。

最先端の暗号技術では、対称と非対称という 2種類のメール暗号化方式があります。いずれも標準的な方式となっており、さまざまなアプリケーションで利用されています。対称鍵暗号とは、送信者と受信者が同じ鍵を共有する暗号化方式です。

一方、非対称鍵暗号(あるいは公開鍵暗号)とは、各ユーザが 2つの暗鍵(データを暗号化する公開鍵と復号化のための秘密鍵(プライベート鍵))を持つ暗号方式です。公開鍵は自由に公開されますが、秘密鍵はユーザが厳重に保管します。

対称暗号方式の欠点として、送信者と受信者が安全に通信するためには、両者があらかじめ鍵を決め、これを互いだけの秘密として維持する必要があります。両者が離れた場所にいる場合、送信中に秘密鍵が開示されないようにしなければなりません。そのため、対称暗号方式では、鍵の受け渡しに関する問題が常に存在します。つまり、「他者に傍受されることなく受信者に鍵を伝えるにはどうすればいいか」という問題です。公開鍵暗号方式は、この問題に対処するために開発されました。公開鍵暗号方式では、ユーザは安全ではないチャネル上でも安全に通信することができ、あらかじめ共有鍵を決める必要はありません。

メール暗号化の必要性から、多種多様な公開鍵暗号化標準が生まれました。最も有名なのは S/MIME と Open PGP であり、Sophos UTMはその両方に対応しています。S/MIME (*Secure Multipurpose Internet Mail Extensions*)とは非対称暗号方式の標準であり、メール署名を MIME にカプセル化します。通常、S/MIME は公開鍵基盤(PKI)内で使用され、デジタル証明の階層構造に基づいており、信頼できるインスタンスとして認証局(CA)を必要とします。CA は、電子鍵のペアを身元情報とバインドして電子証明書を発行します。電子証明書は、パスポートなど従来からある

身分証明書の電子版と考えることができます。技術的に言うと、CA は特定の X.500 *識別名 (DN)* またはメールアドレスなどの *別名* に公開鍵をバインドして証明書を発行します。

デジタル証明書により、任意の鍵を使用する権利を主張する人にその権利があるかどうかを確認することができます。これは、ある人が CA を信頼しており、公開鍵がこの CA によって署名されていることを確認できるのであれば、この人はこの公開鍵が本当に所有者と主張する人のものであると安心できる、という考え方です。

一方、OpenPGP (*Pretty Good Privacy*) は、一般に WOT (*web of trust*) で採用されている非対称暗号方式を使用します。つまり、公開鍵は他のユーザによってデジタル署名され、署名するユーザは署名という行為によって、公開鍵とその人の関連性を保証します。

注 – S/MIME と OpenPGP は類似のサービスを提供しますが、形式は大きく異なります。そのため、一方のプロトコルのユーザは、他方のプロトコルのユーザと通信できません。さらに、認証証明書を共有することもできません。

メール暗号化は、ユーザに対して完全に透過的です。つまり、クライアント側で追加の暗号化ソフトウェアを用意する必要はありません。一般に暗号化では、送信先の証明書または公開鍵が手元にある必要があります。受信メッセージと送信メッセージに対し、メール暗号化機能は次のように機能します。

- デフォルトで、内部ユーザが送信したメッセージはスキャンされ、自動的に署名され、受信者の証明書 (S/MIME) または公開鍵 (OpenPGP) で暗号化されます (受信者の S/MIME 証明書または OpenPGP 公開鍵がUTM上にある場合)。
- UTMが S/MIME 証明書または OpenPGP 公開鍵を認識している外部ユーザから送られてきた暗号化済み受信メッセージは、自動的に復号化され、悪質なコンテンツが含まれないかスキャンされます。メッセージの復号化のためには、内部ユーザの S/MIME 鍵または OpenPGP 秘密鍵がUTMに存在している必要があります。
- UTMが認識できない外部ユーザから送られてきたか、セキュリティシステムが認識できない内部ユーザ向けの暗号化済み受信メッセージは、配達されるものの復号化はできません。従って、ウイルスやスパムのスキャンは行われません。個人用ファイアウォールなどでそのメールにマルウェアが含まれていないことを確認するのは、受信者 (内部ユーザ) の責任となります。
- クライアント側ですでに暗号化されている送信メッセージは、受信者の S/MIME 証明書または OpenPGP 公開鍵が不明な場合、受信者に直接送信されます。一方、受信者の S/MIME 証明書または OpenPGP 公開鍵がわかる場合、メッセージは 2回暗号化されます。あらかじめ暗号化されたメッセージに悪質なコンテンツが含まれないかスキャンすることはできません。

- 復号化が可能なのは受信メールのみです。ここで「受信」と見なされるためには、送信者のメールアドレスのドメイン名が SMTP プロファイルの一部ではないことが条件です。たとえば、jdoe@example.com から送信されたメッセージを復号化するためには、example.com というドメインがルーティング設定またはSMTP プロファイルのいずれにも設定されていないことが求められます。
- 署名/暗号化結果の概要は、各メールの件名行に記述されます。たとえば、あるメールが正しく署名され、S/MIME で暗号化されると、「S/MIME: 署名済み、暗号化済み (Signed and encrypted)」というテキストが件名の行に付加されます。

注 –メールクライアント(例: Microsoft Outlook または Mozilla Thunderbird)が署名済みまたは暗号化済みのメッセージにフッタを追加すると、署名が破壊されて無効になります。デジタル署名をクライアント側で作成する場合は、アンチウイルスチェックフッタオプションを無効にしてください。ただし、メール通信のプライバシーや認証を保ちながら、一般的なウイルス対策チェックフッタを使用する場合は、Sophos UTM の組み込みメール暗号化機能の使用を考慮してください。ゲートウェイ上でのメール暗号化では、デジタル署名を作成する前にフッタがメッセージに付加されるため、署名が損なわれることはありません。

10.4.1 グローバル

*「Eメールプロテクション」>「暗号化」>「グローバル」*タブでは、メール暗号化機能の基本設定を定義することができます。

注 – 暗号化は SMTP のみで機能し、POP3 では機能しません。

メール暗号化を使用するためには、CA 証明書と CA 鍵から成る*認証局*(CA)を作成しておく必要があります。CA 証明書はダウンロードしてローカルに保存することができます。さらに、図で示すように、他のユニットに外部 CA (S/MIME 認証局)としてインストールし、2つのSophos UTMユニット間で透過的なメール暗号化を実現することもできます。

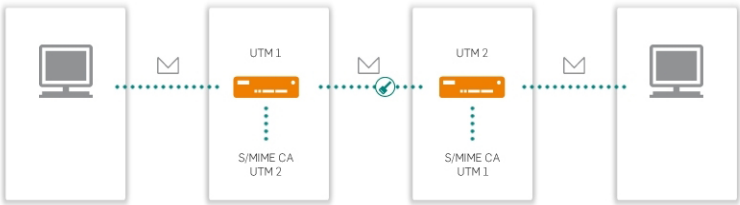

Figure 19 メール暗号化:2つのSophos UTMユニットの使用

メール暗号化を設定するには、次の手順に従ってください。

1. **「*グローバル*」タブで、メール暗号化を有効化します。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*メール暗号化認証局 (CA)*」エリアが編集可能になります。

2. **認証局 (CA) を作成します。**
   「*メール暗号化認証局 (CA)*」エリアのフォームに記入します。デフォルトで、このフォームには「*マネジメント > システム設定 > 組織*」タブの値が入力されています。

3. **「*保存*」をクリックします。**
   トグルスイッチが緑色になり、次の証明書と鍵が作成されます。

   - S/MIME CA 証明書
   - OpenPGP ポストマスタ鍵

   これが完了するまで数分かかる可能性があります。S/MIME CA 証明書または OpenPGP ポストマスタ鍵のフィンガープリントが表示されない場合、WebAdmin の右上隅にある「*リロード*」ボタンをクリックしてください。証明書と鍵は、ダウンロードしてローカルに保存できます。

「*暗号化*」メニューのすべての設定を工場出荷時のデフォルト設定にリセットするには、「*メール暗号化システムを今すぐリセット*」ボタンを使用します。

10.4.2 オプション

「*暗号化 > オプション*」タブでは、Sophos UTMの公開鍵暗号フレームワーク内で使用されるデフォルトポリシーを定義できます。

デフォルトポリシー:メールの暗号化に関するデフォルトポリシーを指定します。これらの設定は、カスタマイズされた設定で上書きできます。

次の作業を実行できます。

- 送信メールに署名
- 外部宛送信メールの暗号化
- 内部宛受信メールの検証
- 受信メールの複合化

設定を保存するには「*適用*」をクリックします。

注 – 暗号化が機能するためには、送信者が「*内部ユーザ*」リストに含まれている必要があります。S/MIME 証明書または OpenPGP 公開鍵がゲートウェイに存在する受信者に向けた送信メールは、デフォルトで暗号化されます。これらの受信者に対する暗号化を無効にするには、当該受信者の S/MIME 証明書または OpenPGP 公開鍵を削除してください。証明書または公開鍵がUTMに不明の場合、メールは暗号化されずに送信されます。

S/MIME 証明書の自動抽出

このオプションを選択すると、S/MIME 証明書は受信メールから自動的に抽出されます。このとき、そのメールに添付された証明書が、信頼される認証局に署名されていることが条件となります。信頼される認証局とは、*「Eメールプロテクション」>「暗号化」>「S/MIME 認証局」*タブに表示される、ユニットにある CA です。さらに、証明書の自動抽出が機能するためには、Sophos UTMの時間と日付が、証明書の有効期間内である必要があります。証明書の抽出が成功すると、証明書は「*Eメールプロテクション > 暗号化 > S/MIME 証明書*」タブに追加されます。これが完了するまで 5～10分かかる可能性があります。設定を保存するには「*適用*」をクリックします。

OpenPGP 鍵サーバ

OpenPGP 鍵サーバは公開 PGP 鍵をホストします。ここで、OpenPGP 鍵サーバを追加することができます。署名された受信メールや暗号化する送信メールで、該当する公開鍵がUTMに不明の場合、UTMは所与のサーバから公開鍵を取得しようとします。

10.4.3 内部ユーザ

メッセージの署名と復号化を行うためには、S/MIME 鍵またはOpenPGP 秘密鍵がUTMに存在している必要があります。「*暗号化 > 内部ユーザ*」タブでは、メール暗号化を有効にするユーザに対して、個別の S/MIME 鍵/証明書または OpenPGP 鍵ペア（あるいはその両方）を作成できます。

内部メールユーザを作成するには、次の手順に従います。

1. **「*内部ユーザ*」タブで「*新規メール暗号化ユーザ*」をクリックします。**
   「*新規ユーザの作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   メールアドレス:ユーザのメールアドレスを入力します。

   フルネーム:ユーザの名前を入力します。

   署名:以下の署名オプションを利用できます。

- デフォルトポリシーを使用:「*オプション*」タブのポリシーが使用されます。
- オン:メールは、ユーザの証明書を使用して署名されます。
- オフ:メールは署名されません。

暗号化:以下の暗号化オプションを利用できます。

- デフォルトポリシーを使用:「*オプション*」タブのポリシーが使用されます。
- オン:メールは、受信者の公開鍵を使用して暗号化されます。
- オフ:メールは暗号化されません。

確認中:以下の検証オプションを利用できます。

- デフォルトポリシーを使用:「*オプション*」タブのポリシーが使用されます。
- オン:メールは、送信者の公開鍵を使用して検証されます。
- オフ:メールは検証されません。

復号化:以下の復号化オプションを利用できます。

- デフォルトポリシーを使用:「*オプション*」タブのポリシーが使用されます。
- オン:メールは、ユーザの証明書を使用して復号化されます。
- オフ:メールは復号化されません。

S/MIME:S/MIME 証明書と鍵をシステムに自動生成させるか、証明書を PKCS#12 形式でアップロードするかを選択します。証明書をアップロードする場合、PKCS#12 ファイルの保護に使用されたパスフレーズを知っている必要があります。PKCS#12 ファイルには、S/MIME 鍵と証明書の両方が含まれていなければなりません。この PKCS#12 ファイルに含まれているすべての CA 証明書は無視されます。

OpenPGP:秘密鍵と公開鍵から成る OpenPGP 鍵ペアをシステムに自動生成させるか、鍵ペアを ASCII 形式でアップロードするかを選択します。秘密鍵と公開鍵の両方が 1つのファイルに格納されており、ファイルにパスフレーズが含まれていないことが必要です。

注 – あるユーザに対して S/MIME と OpenPGP の両方が設定されている場合、このユーザから送信されるメールの署名と暗号化は S/MIME を使用して行われます。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
新しいユーザが「*内部ユーザ*」リストに表示されます。

トグルスイッチを使用して、いずれかの鍵（または両方）の使用をオフにします。鍵を削除する必要はありません。

注 – セキュリティ上の理由から、ダウンロード用に提供されたそれぞれのファイルには S/MIME 証明書と OpenPGP 公開鍵のいずれかのみが含まれています。S/MIME 鍵と OpenPGP 秘密鍵はシステムからダウンロードできません。

10.4.4 S/MIME 認証局

「*暗号化 > S/MIME 認証局*」タブでは、メール暗号化用の認証局（CA）を管理できます。事前にインストール済みの CA 以外にも、外部証明機関の証明書をアップロードすることもできます。このリスト内の CA のいずれかに署名され、有効化された証明書を含むすべての受信メールは、自動的に信頼されます。

注 – *「Eメールプロテクション」>「暗号化」>「オプション」*タブで*「自動 S/MIME 証明書抽出の有効化」*オプションを選択した場合は、ここにリストされた CA によって署名され、有効化された証明書は、自動的に抽出され、*「Eメールプロテクション」>「暗号化」>「S/MIME 証明書」*タブに配置されます。

ローカル S/MIME 認証局

信頼する外部認証局の証明書（つまり公開鍵）をインポートします。これにより、この CA が証明書に署名したすべての受信メールについても信頼することになります。たとえば、他の Sophos UTM ユニットの CA をインストールすると、2つの Sophos UTM ユニット間でメールを透過的に暗号化することができます。

外部 S/MIME 認証局の証明書をインポートするには、次の手順に従います。

1. **「*ローカル CA をアップロード*」フィールドの横のフォルダアイコンをクリックします。**
   「*ファイルのアップロード*」ダイアログボックスが開きます。
2. **アップロードする証明書を選択します。**
   「*参照*」をクリックして、アップロードする CA 証明書を選択します。次の証明書の拡張子がサポートされています。
   - `cer`、`crt`、または `der`:これらの証明書タイプはバイナリで、基本的には同じです。
   - `pem`:Base64 で暗号化された DER 証明書。
3. **証明書をアップロードします。**
   「*アップロード開始*」をクリックして、選択した CA 証明書をアップロードします。

証明書はインストールされ、「*ローカル S/MIME 認証局*」エリアに表示されます。

CA を信頼できない場合は、S/MIME 認証局の証明書を削除または無効化できます。S/MIME 認証局の証明書を無効にするには、トグルスイッチをクリックします。トグルスイッチが灰色になり、SMTP プロキシはこの S/MIME 認証局に署名されたメールを受け入れなくなります。証明書を削除するには、空にするアイコンをクリックします。

ヒント – CA のフィンガープリントを表示するには、青色の情報アイコンをクリックしてください。

グローバル S/MIME 認証局

ここに表示される S/MIME CA のリストは、Mozilla Firefox にあらかじめインストールされた S/MIME CAと同じです。これにより、これらの CA に基づいて PKI を管理しているコミュニケーションパートナーとお客様の間で、メールの暗号化が促進されます。CA を信頼できない場合は、S/MIME 認証局の証明書を無効化できます。S/MIME 認証局の証明書を無効にするには、トグルスイッチをクリックします。トグルスイッチが灰色になり、SMTP プロキシはこの S/MIME 認証局に署名されたメールを受け入れなくなります。

次のリンクは、有名なルート証明書の URL です。

- Trustcenter
- S-TRUST
- Thawte
- VeriSign
- GeoTrust

10.4.5 S/MIME 証明書

「*暗号化 > S/MIME 証明書*」タブでは、外部 S/MIME 証明書をインポートすることができます。証明書がここにリストされている受信者へのメールは自動的に暗号化されます。特定の受信者に対する暗号化を無効にするには、リストから証明書を削除してください。

注 – 受信者に対し、S/MIME 証明書に加えて OpenPGP 公開鍵がインポートされた場合、メールは OpenPGP で暗号化されます。

注 – S/MIME 証明書を手動でアップロードすると、証明書に記載された人を識別できる CA 証明書がなくても、証明書に関連付けられたメールアドレスからのメッセージが常に信頼されるよう

になります。つまり、S/MIME 証明書を手動アップロードするということは、送信元に「信頼できる」というラベルを貼り付けるということになります。

外部 S/MIME 証明書をインポートするには、次の手順に従います。

1. **「*S/MIME 証明書*」タブで「*新規外部 S/MIME 証明書*」をクリックします。**
「*S/MIME 証明書の追加*」ダイアログボックスが開きます。
2. **次の設定を行います。**
フォーマット:証明書の形式を選択します。次の形式を選択できます。
   - `der`(バイナリ)
   - `pem`(ASCII)

   注 – Microsoft Windows オペレーティングシステムでは、`der` 形式と `pem` 形式の両方に対してファイル拡張子 `cer` を使用します。そのため、アップロードする証明書をバイナリ形式にするか ASCII 形式にするかを、あらかじめ決定しておく必要があります。次に、これに従ってドロップダウンリストで形式を選択します。

   証明書:フォルダアイコンをクリックして、「*ファイルのアップロード*」ダイアログウィンドウを開きます。ファイルを選択し、「*アップロード開始*」をクリックします。

   コメント(任意):説明などの情報を追加します。
3. **「*保存*」をクリックします。**
新しい S/MIME 証明書が「*S/MIME 証明書*」リストに表示されます。

10.4.6 OpenPGP 公開鍵

「*暗号化 > OpenPGP 公開鍵*」タブでは、OpenPGP 公開鍵をインストールすることができます。`.asc` 形式のファイルを提供する必要があります。鍵束全体のアップロードがサポートされています。

注 – パスフレーズで保護されている鍵束ファイルはアップロードしないでください。

この鍵束ファイルに含まれるすべての公開鍵がインポートされ、メッセージの暗号化に使用できるようになります。公開鍵がここにリストされている受信者へのメールは自動的に暗号化されます。特定の受信者に対する暗号化を無効にするには、リストから公開鍵を削除してください。

注 – 鍵ごとに1つのメールアドレスだけがサポートされます。1つの鍵に複数のアドレスが関連付けられている場合、「最初の」アドレスのみが使用されます(この順序は、OpenPGP のアドレスのソート方法に応じています)インポートしたい鍵に複数のアドレスが関連付けられている場合、その鍵をSophos UTMにインポートする前に、OpenPGP またはその他のツールで不要なアドレスを削除する必要があります。

OpenPGP 公開鍵をインポートするには、次の手順に従います。

1. **「*OpenPGP 公開鍵*」タブで、「*OpenPGP鍵束ファイルのインポート*」をクリックします。**
   「*OpenPGP 鍵束ファイルをインポート*」ダイアログボックスが開きます。
2. **OpenPGP 鍵をアップロードします。**
   フォルダアイコンをクリックして、「*ファイルのアップロード*」ダイアログウィンドウを開きます。ファイルを選択し、「*アップロード開始*」をクリックします。

   鍵または鍵のリスト(ファイルに複数の鍵が含まれている場合)が表示されます。
3. **鍵を1つ以上選択し、「*選択した鍵をインポート*」をクリックします。**
   鍵が「*OpenPGP 公開鍵*」リストに表示されます。

注 – 鍵にはメールアドレスが 1つ関連付けられていなければならず、関連付けられていない場合、インストールは失敗します。

10.5 隔離レポート

Sophos UTM Sophos UTM は、さまざまな理由からブロックされて隔離場所にリダイレクトされたすべてのメッセージ(SMTP および POP3)を含むメールの隔離場所を用意しています。ここには、配信待ちのメッセージ、悪意あるソフトウェアに感染したメッセージ、疑わしい添付ファイルを含むメッセージ、スパムと特定されたもの、または単に不要な表現を含むメッセージが含まれます。

メッセージが間違って隔離されて保留されるリスク(いわゆる*誤検出*)を最小限に抑えるために、Sophos UTMは、隔離されたメッセージについて報告する隔離レポートをユーザに毎日送信します。ユーザに複数のメールアドレスが設定されている場合は、それぞれのメールアドレスに個々の隔離レポートが送信されます。ユーザポータルで追加の POP3アカウントが設定されており、Sophos UTM の POP3プロキシが*プリフェッチモード*(POP3 サーバからメッセージをプリフェッチし、ローカルデータベースに保存することが可能)である場合にも、これは適用されます。隔離レポートでは、ユーザはスパムエントリをクリックしてメッセージを隔離場所からリリースしたり、今後のために送信者をホワイトリストに追加できます。

隔離レポートの詳細について、以下に少し説明します。

- 隔離レポートは、メールアドレスが SMTP プロファイルに含まれているドメインの一部であるユーザに対してのみ送信されます。隔離レポートには、「*SMTP > ルーティング(Routing)*」タブの「*ドメイン*」ボックスで指定したものや、SMTPプロファイルの「*ドメイン*」ボックスで指定したものが含まれます。
- POP3 *プリフェッチオプション*が無効の場合、このアカウントに送信された隔離されたメッセージは隔離レポートには表示されません。代わりに、各ユーザの受信トレイに、一般的な Sophos POP3 のブロックメッセージが表示されます。したがって、隔離レポートまたはユーザポータルを使用してメッセージをリリースすることはできません。このようなメールは、管理者が zip 形式でメールマネージャからダウンロードすることでのみ配信できます。
- 「*詳細*」タブで、管理者は、ユーザがリリースできる隔離メールのタイプを定義します。デフォルトでは、隔離場所からリリースできるのは、スパムメールだけです。他の理由で隔離されたメッセージ(ウイルスや疑わしい添付ファイルを含むメッセージなど)は、Sophos UTMのメールマネージャで管理者によってのみ隔離場所からリリースできます。さらに、ユーザは、現在隔離されているすべてのメッセージをSophosユーザポータルで確認することができます。
- スパムメールに複数の受信者がいる場合は、メーリングリストの場合と同様に、受信者の誰かがそのメールをリリースすると、メーリングリストのメールアドレスがシステムで設定されている場合は、そのメールはその受信者のみにリリースされます。そうでない場合は、そのメールはすべての受信者に同時に配信されます。詳細は、「*Eメールプロテクション > 隔離レポート > 除外*」タブの「*内部メーリングリストの定義*」オプションを参照してください。
- 管理者は、Sophos UTMでユーザが設定されていない SMTP メールアドレスに送信されたメールを、隔離レポートまたはメールマネージャからリリースできます(ホワイトリストへの追加はしない)。ただし、このユーザが設定されていないため、ユーザポータルへのアクセスはできません。
- メーリングリストに送信されたスパムメールはホワイトリストに追加できません。
- メールクライアントでメールのヘッダを正しくエンコードしないとデイリーの隔離レポートのメールが正しく表示されない場合があります。

10.5.1 グローバル

「*隔離レポート > グローバル*」タブで、デイリーの隔離レポートの送信時刻を定義して、隔離レポートに表示されるメッセージテキストを記述できます。

隔離レポートの設定を編集するには、隔離レポートを有効にします。トグルスイッチをクリックします。
トグルスイッチが緑色に変わります。

レポート送信時刻

ここでデイリーの隔離レポートの送信時刻を定義できます。ドロップダウンリストで時刻を選択し、「*適用*」をクリックします。
追加のレポートを送信することもできます。これを行うには、「*追加のレポートを送信*」チェックボックスにチェックを入れ、時刻を設定して、「*適用*」をクリックします。

カスタマイズ可能なメッセージテキスト

ここで、隔離レポートの序文となるテキストをカスタマイズできます。必要に応じてメッセージテキストを変更して、「*適用*」をクリックします。

注 – カスタマイズ可能なメッセージテキストボックスでは HTML タグは使用できません。

注 – ホームユーザライセンスを使用している場合は、カスタマイズできません。

10.5.2 除外

「*隔離レポート > 除外*」タブで、デイリーの隔離レポートの受信から除外するメールアドレスのスキップリストを定義できます。

隔離レポートのスキップ

ここで隔離通知を送信しない内部メールアドレスを設定できます。ここにメールアドレスがリストされているユーザは、デイリーの隔離レポートを受信しません。完全なメールアドレスを入力するか、または `*@example.com` のようにアスタリスク(*)をワイルドカードどして使用できます。

注 – スキップリストは SMTP 隔離レポートにのみ適用されます。それぞれのユーザに指定された POP3 アカウントがある場合は、POP3 隔離レポートはそれにもかかわらず送信されます。

内部メーリングリストの定義

メーリングリストのメールアドレスが「*メーリングリストアドレスパターン*」ボックスで設定されている場合に(例: `newsletter@example.com`)、このメーリングリストに送信されたスパムメッセージが検知されてメールの隔離場所にリダイレクトされたときは、このメーリングリストに含まれるすべての受信者の隔離レポートがこのスパムメッセージへのリンクを含みます。したがって、各受信者は、受信者が隔離レポートの「*リリース*」リンクをクリックすると表示されるユーザプロンプトに自身のメールアドレスを入力することで、このスパムメッセージを個々にリリースできます。

注 – メーリングリストは隔離レポートまたはユーザポータルでホワイトリスト化できません。

代わりに、特定メーリングリストのメールアドレスを、追加メールアドレスとしてローカルユーザのプロファイルに入力することで、このユーザを一種のメールマネージャに設定できます。すると、このユーザの隔離レポートのみがメーリングリストに送信されたスパムメッセージへのリンクを含むようになります。「*リリース*」リンクをクリックすると、そのメーリングリストのすべての受信者に一度にスパムメッセージが送信されます。

注 – メーリングリストのメールアドレスがユーザのプロファイルの追加メールアドレスとして設定されている場合は、そのメーリングリストに送信されたスパムメッセージへのリンクは、そのメーリングリストの受信者には表示されません。

ただし、メーリングリストのメールアドレスがユーザのプロファイルおよび「*メーリングリストアドレスパターン*」ボックスの両方で追加メールアドレスとして設定されている場合は、そのユーザの隔離レポートの「*リリース*」リンクからユーザプロンプトが開きます。そこでスパムメッセージの転送先のそれぞれのメールアドレスを手動で入力して、スパムメールの受信者を決定できます。

最後に、メーリングリストのメールアドレスがユーザプロファイルとメーリングリストアドレスパターンのどちらでも追加メールアドレスとして設定されていない場合は、メーリングリストに送信されたスパムメッセージは通常のメールのように扱われます。つまり、受信者の誰かがスパムメールをリリースすると、それはメーリングリストのすべての受信者に送信されます。

要約すると、メーリングリストのメールアドレスをメーリングリストアドレスパターンとして設定すると、隔離レポートにスパムメッセージへのリンクを持つ各ユーザは、スパムメッセージのリリース先のメールアドレスを入力するように要求されることになります。

10.5.3 詳細

「*隔離レポート > 詳細*」タブで、デイリーの隔離レポートに含まれる「*リリース*」リンクに代替ホスト名とポート番号を設定できます。また、スパムメールのリリースオプションを変更することもできます。

隔離レポート詳細オプション

ホスト名:デフォルトでは、「*マネジメント*」>「*システム設定*」>「*ホスト名*」タブのゲートウェイのホスト名です。ゲートウェイが送信する隔離レポートには、ハイパーリンクなどが含まれており、ユーザはこれをクリックしてメール隔離場所からメッセージをリリースできます。デフォルトでは、これらのリンクはここで指定したホスト名をポイントしています。ユーザがインターネット上でメールをリリースできるようにしたい場合は、パブリックに解決できる代替ホスト名をここに入力する必要があります。

ポート:デフォルトでは、ポート `3840` が設定されています。ポートは、`1024`～`65535` の範囲内でどの値にでも変更できます。

許可ネットワーク:メールリリースサービスへの接続を許可するネットワークも指定できます。デフォルトでは、内部ネットワークのみが選択されています。

設定を保存するには「*適用*」をクリックします。

リリースオプション

ここで、ユーザがリリース可能な隔離メッセージのタイプを選択できます。以下のオプションから選択できます。

- マルウェア
- スパム
- 表現フィルタ
- ファイル拡張子
- スキャン不可
- MIME タイプ
- その他

設定を保存するには「*適用*」をクリックします。

10.6 メールマネージャ

メールマネージャとは、機器に現在保存されているすべてのメールメッセージを管理および整理するための管理ツールです。配信待ちのメッセージや、悪意あるソフトウェアに感染している隔離メッセージ、疑わしい添付ファイルが添付されている隔離メッセージ、スパムとして識別された隔離メッセージ、または好ましくない表現が含まれている隔離メッセージなどが表示されます。メッセージをダウンロード、リリース、削除する前に、メールマネージャを使用してすべてのメッセージをレビューすることができます。メールマネージャは UTF-8 に完全に対応しています。

10.6.1 メールマネージャウィンドウ

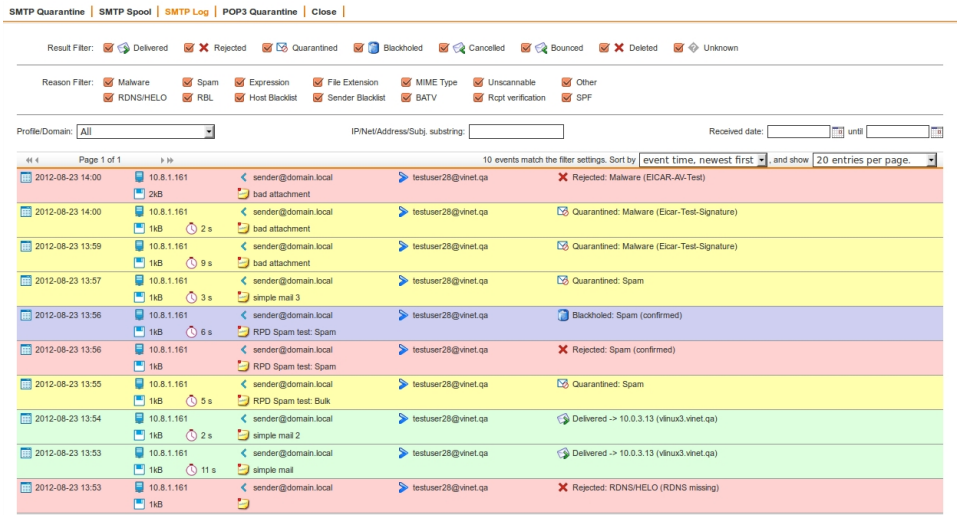

Figure 20 メールマネージャ – Sophos UTM

「メールマネージャ」ウィンドウを開くには、「*Eメールプロテクション > メールマネージャ > グローバル*」タブの「*新しいウィンドウでメールマネージャを開く*」ボタンをクリックします。メールマネージャは、次の5つのタブに分割されています。

- **SMTP Quarantine:**現在隔離されているすべてのメッセージを表示します。
- **SMTP Spool:**現在 `/var/spool` にあるすべてのメッセージを表示します。これらのメッセージは、配信待ちであるか、エラーが発生したためにスプールに含まれている可能性があります。
- **SMTP Log:**SMTP 経由で処理されたすべてのメッセージの配信ログを表示します。
- **POP3 Quarantine:**POP3 経由で取得され、現在隔離されているすべてのメッセージを表示します。
- **閉じる:**これをクリックすると、メールマネージャウィンドウが閉じます。

10.6.1.1 SMTP/POP3 隔離

SMTP および POP3 隔離内のメッセージは、それぞれの隔離理由別に表示することができます。

- マルウェア
- スパム
- 表現ブロック
- ファイル拡張子
- MIME タイプ（SMTP のみ）
- スキャン不可
- その他

チェックボックスを使用して、隔離理由を選択/選択解除します。隔離理由のチェックボックスをダブルクリックすると、この理由だけが選択されます。

ヒント – メッセージを表示するには、メッセージをダブルクリックします。

Profile/Domain（プロファイル/ドメイン）:プロファイル/ドメインを選択すると、そのプロファイル/ドメインのメッセージのみが表示されます。

Sender/Rcpt/Subject substring（送信者/受信者/件名サブストリング）:ここでは、メッセージ内で検索する送信者、受信者、または件名を入力します。

Received date（受信日）:特定の期間内に処理されたメッセージのみを表示するには、日付を入力するか、カレンダーアイコンで日付を選択します。

Sort by（ソート順）:デフォルトでは、受信時刻によりリストがソートされています。ここでは、別のソート基準を選択できます。

and show（表示）:チェックボックスを選択することで、1ページあたり 20件、50件、100件、250件、500件、1000件、またはすべてのメッセージを表示することができます。すべてのメッセージの表示には時間がかかる場合があります。

各メッセージの前にあるチェックボックスを使用するか、メッセージをクリックして、選択したメッセージにアクションを適用します。次の作業を実行できます。

- **Download（ダウンロード）:**選択されたメッセージをダウンロードします。
- **Delete（削除）:**選択されたメッセージを削除します。これを取り消すことはできません。
- **Release（リリース）:**選択されたメッセージを隔離からリリースします。
- **Release and report as false positive（リリースし、誤検出として報告）:**選択したメッセージを隔離からリリースし、スパムスキャンエンジンに誤検出として報告します。

隔離に保留されているメッセージをすべてリリースできるのは管理者だけです。Sophosユーザポータルでメッセージを確認するユーザは、明示的に許可されているメッセージのみをリリースすることができます。この権限付与設定は、*「Eメールプロテクション」>「隔離レポート」>「詳細」*タブで確認できます。

Select action to apply on message(s)(グローバルクリーンアップアクションの選択):ここには、メッセージに対してグローバルに適用されるさまざまな削除オプションがあります。つまり、選択されていないメッセージや表示されていないメッセージにもオプションが適用されます。

警告 – メッセージの削除を取り消すことはできません。

10.6.1.2 SMTP Spool

ここには、配信待ちメッセージまたはエラーが発生したメッセージが表示されます。配信ログは、メッセージヘッダの一部でもあります。次のチェックボックスを使用して、表示するメッセージのタイプを1つだけ選択してください。

- **Waiting**:配信待ちのメッセージ。
- **Error**:エラーが発生したメッセージ。あるメッセージでエラーが複数回発生した場合は、Sophosパートナーまたは Sophosサポートチームに報告してください。

ヒント – メッセージを表示するには、メッセージをダブルクリックします。

Profile/Domain(プロファイル/ドメイン):プロファイル/ドメインを選択すると、そのプロファイル/ドメインのメッセージのみが表示されます。

Sender/Rcpt/Subject substring(送信者/受信者/件名サブストリング):ここでは、メッセージ内で検索する送信者、受信者、または件名を入力します。

Received date(受信日):特定の期間内に処理されたメッセージのみを表示するには、日付を入力するか、カレンダーアイコンで日付を選択します。

Sort by(ソート順):デフォルトでは、受信時刻によりリストがソートされています。ここでは、別のソート基準を選択できます。

and show(表示):チェックボックスを選択することで、1ページあたり 20件、50件、100件、250件、500件、1000件、またはすべてのメッセージを表示することができます。すべてのメッセージの表示には時間がかかる場合があります。

各メッセージの前にあるチェックボックスを使用するか、メッセージをクリックして、選択したメッセージにアクションを適用します。次の作業を実行できます。

- **Download(ダウンロード):**選択されたメッセージをダウンロードします。
- **Retry(再試行):**選択されたメッセージの配信を即時に再試行します。
- **Delete(削除):**選択されたメッセージを削除します。これを取り消すことはできません。
- **Bounce(バウンス):**選択されたメッセージをバウンスします。送信者には、メッセージの配信がキャンセルされたことを伝えるメッセージが送信されます。

グローバルクリーンアップアクションの選択:ここには、メッセージに対してグローバルに適用されるリトライオプションやいくつかの削除オプションがあります。つまり、選択されていないメッセージや表示されていないメッセージにもオプションが適用されます。

警告 – メッセージの削除を取り消すことはできません。

10.6.1.3 SMTP ログ

「*SMTP Log*」には、SMTP 経由で処理されたすべてのメッセージのログメッセージが表示されます。

Result Filter(結果フィルタ):表示されるメッセージのタイプを選択するには、該当するチェックボックスにチェックを入れます。

- **Delivered(配信済み):**配信が成功したメッセージ。
- **Rejected(リジェクト):**UTMに拒否されたメッセージ。
- **Quarantined(隔離):**隔離されたメッセージ。
- **Blackholed(ブラックホール; 削除済み):**通知なしで削除されたメッセージ。
- **Canceled(キャンセル):***SMTP スプール*に手動でバウンスされたメッセージ。
- **Bounced(バウンス):**ルーティング設定が正しくないなどの理由により、配信できないメッセージ。
- **Deleted(削除済み):**手動で削除されたメッセージ。
- **Unknown(不明):**ステータスが不明なメッセージ。

「*結果フィルタ*」アイテムの選択/選択解除を切り替えるには、チェックボックスを使用します。アイテムをダブルクリックすると、そのアイテムだけが選択されます。

Reason Filter(理由フィルタ):メッセージログの表示をさらにフィルタするには、チェックボックスを使用します。

ヒント – メッセージログを表示するには、メッセージログをダブルクリックします。IP アドレスを解決するには、メッセージのサーバアイコンをクリックします。アスタリスク (*) は、リバース DNS ルックアップが成功したことを示します。

Profile/Domain(プロファイル/ドメイン):プロファイル/ドメインを選択すると、そのプロファイル/ドメインのメッセージのみが表示されます。

IP/Net/Address/Subj. substring(IP/ネット/アドレス/件名 サブストリング):ここでは、SMTP ログメッセージ内で検索する IP アドレス、ネットワークアドレス、または件名を入力します。

Received date(受信日):特定の期間内に処理されたメッセージのみを表示するには、日付を入力するか、カレンダーアイコンで日付を選択します。

Sort by(ソート基準):メッセージは、イベント時間、送信者アドレス、メッセージサイズを基準にソートできます。

and show(表示数):表示するエントリ数として、1ページあたり 20エントリ、50エントリ、100エントリ、250エントリ、500エントリ、1000エントリ、またはすべてのメッセージを選択することができます。すべてのメッセージの表示には時間がかかる場合があります。

10.6.2 グローバル

「*メールマネージャ > グローバル*」タブの上部では、「*新しいウィンドウでメールマネージャを開く*」ボタンをクリックしてメールマネージャを開くことができます。

下部にある「*統計概観*」エリアには、ユニットに現在保存されているすべてのメッセージの概要が表示されます。データは SMTP プロトコル経由か POP3 プロトコル経由かによって分類されています。両方のタイプに対して、次の情報が表示されます。

- **配信待ち(スプール中)**(SMTP のみ):スキャン中なのでまだ配信できないなどの理由により、現在スプールにあるメール。
- **クリーンメール総数** (POP3 のみ):ユニットがプリフェッチし、クライアント/ユーザがまだ回収していないメール。
- **隔離マルウェア**:ウイルスやその他の危険なコンテンツなどのマルウェアを含むメッセージの総数。
- **隔離スパム**:スパムと特定されたメッセージの総数。
- **表現ブロックによる隔離**:許可されない表現が含まれるために隔離に移されたメッセージの総数。

- **ファイル拡張子による隔離**:疑わしい添付ファイルが含まれるために隔離されたメッセージの総数(ファイル拡張子で識別)。
- **スキャン不可のため隔離**:スキャンできないため隔離されたメッセージの総数。
- **MIMEタイプによる隔離**(SMTP のみ):SMTP 設定に従ってフィルタすべき MIME タイプが含まれるため隔離されたメッセージの総数。
- **総隔離数**:隔離されたメッセージの総数。

注 – 「*配信待ち*」の数は、SMTP メッセージの場合はリアルタイムのスナップショットを表します。ただしPOP3メッセージの場合は、表示される数は、前回プリフェッチが有効にされたときからの累積数です。

下に、過去 24時間以内の SMTP 隔離および拒否(リジェクト)の簡単な統計が表示されます。

- **マルウェア隔離/リジェクト**:有害なコンテンツが含まれるため隔離/拒否されたメッセージの数。
- **スパム隔離/リジェクト**:スパム認定されたため隔離/拒否されたメッセージの数。
- **ブラックリストリジェクト**:送信者がブラックリストに含まれているため拒否されたメッセージの数。
- **アドレス検証リジェクト**:送信者アドレスを検証できなかったため拒否されたメッセージの数。
- **SPF リジェクト**:送信ホストが許可されないため拒否されたメッセージの数。
- **RBL リジェクト**:送信者がリアルタイムブラックホールリストに含まれているため拒否されたメッセージの数。
- **BATV リジェクト**:BATV タグを検証できなかったために拒否されたメッセージの数。
- **RDNS/HELO リジェクト**:HELO が無効であるか RDNS エントリが不足しているために拒否されたメッセージの数。

拒否があるかどうかは「*Eメールプロテクション > SMTP*」での設定に依存します。

10.6.3 設定

「*メールマネージャ > 設定*」タブでは、データベースログをどれくらいの期間保存するのか、そして隔離メッセージを何日後に隔離場所から削除するのかを設定することができます。有効期限設定の日数を超えたログとメッセージは自動的に削除されます。

デフォルト設定は次のとおりです。

- データベースログは 3日経過後に削除されます。許可される最大日数:30日。
- 隔離メッセージは 14日経過後に削除されます。許可される最大日数:999日。

データベースログと隔離の両方に対して許可される最低日数は 1日です。

データベースログのクリア

このオプションは、データベースログに大量のデータが蓄積された場合にログを即時消去するときに便利です。これを使用すれば、通常のクリーンアップアクションが実行されるまで待つ必要はありません。

11 エンドポイントプロテクション

「*Endpoint Protection*」(エンドポイントプロテクション)メニューでは、デスクトップコンピュータ、サーバ、モバイル PC など、ネットワーク上のエンドポイントデバイスの保護を管理できます。UTMここでは、エンドポイントソフトウェアの導入、保護対象のエンドポイントの概要確認、エンドポイントのグループ化、アンチウイルスおよびデバイスコントロールポリシーの設定、定義したポリシーのエンドポイントグループへの割り当てを行います。

エンドポイントプロテクションでは、Sophos LiveConnect と呼ばれるセンターサービスを使用しています。このクラウドベースのサービスは、エンドポイントプロテクション機能を有効にした段階で、UTMに使用できるように自動的にセットアップされます。LiveConnect を使用すると、ローカルネットワークに存在するかどうかに関係なく、リモートサイトや外出の多いユーザのエンドポイントを含め、常にすべてのエンドポイントを管理できます。LiveConnect サービスは以下を提供します。

- エンドポイントエージェント用の設定済みインストールパッケージ
- エンドポイントに対するポリシーの導入および更新
- エンドポイントのセキュリティ更新および定義
- WebAdmin によりエンドポイントを集中管理でモニタリングするための中央でのログ記録とデータレポート

LiveConnect はクラウドベースのサービスであるため、サービスを機能させるためには、アクティブなインターネット接続が必要になります。管理対象のエンドポイントにも、ポリシーおよびセキュリティ更新を受信するためのインターネット接続が必要になります。

次の図は、LiveConnect サービスを使用したSophos UTMエンドポイントプロテクションの導入例を示します。

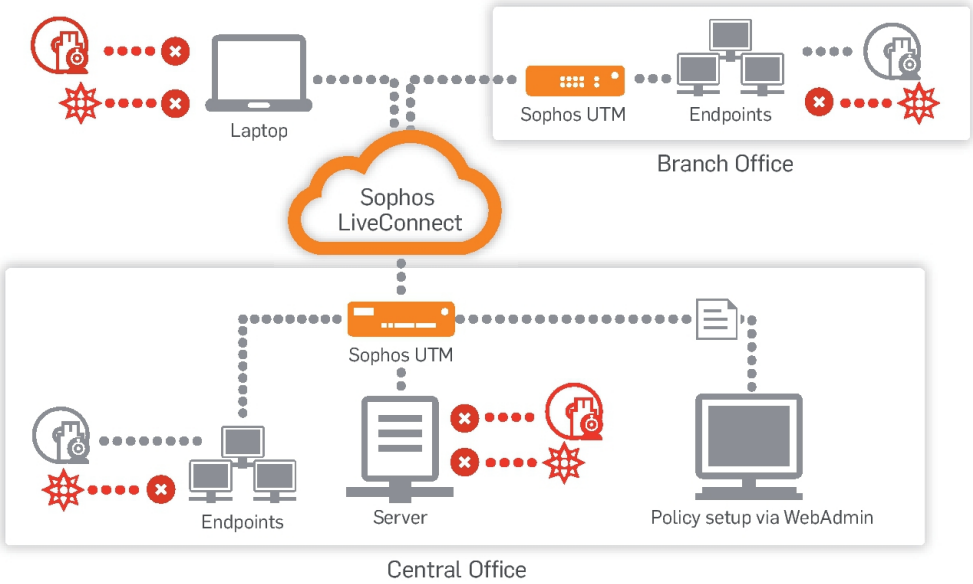

Figure 21 エンドポイントプロテクション:概要

この章では、次のトピックについて説明します。

- コンピュータ管理
- アンチウイルス
- デバイスコントロール

エンドポイントプロテクションを有効にすると、登録されているコンピュータの全般的な情報とステータスを概要ページで確認できます。リストのソートと検索ができます。エンドポイントのステータスがでない場合 *Ok*、ステータスをクリックすることでウインドウが開き追加の情報を得ることができます。ステータスが *適合しない場合は*、そのデバイスの設定が設定したものと異なっていることを示しますUTM。この問題を解決するために、ウィンドウ中のリンクから現在の設定をエンドポイントへ送ることができます。その他のステータス対しても、どのようなアクションが必要かといった情報を得ることができます。

エンドポイントプロテクションライブログを開く

エンドポイントプロテクションライブログはエンドポイントとLiveConnect との接続に関する情報を示します。さらにUTM、エンドポイントのセキュリティに関する情報も示します。「*エンドポイントプロテク*

ションライブログを開く」ボタンをクリックすると、新しいウィンドウでエンドポイントプロテクションライブログが開きます。

11.1 コンピュータ管理

「*エンドポイントプロテクション > コンピュータ管理*」ページでは、Sophos UTMに接続された個々のコンピュータの保護を管理することができます。

ここでは、エンドポイントのインストールファイルを検索して導入したり、エンドポイントプロテクションソフトウェアがインストールされているすべてのコンピュータの概要を確認することができます。さらに、コンピュータグループごとに、異なる保護を設定できます。

11.1.1 グローバル

「*エンドポイントプロテクション > コンピュータ管理 > グローバル*」タブでは、エンドポイントプロテクションを有効または無効にできます。

エンドポイントプロテクションを有効にするには、次の手順に従います。

1. **「*グローバル*」タブで、エンドポイントプロテクションを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、組織の詳細に関するフィールドが表示されます。

2. **組織の詳細を入力します。**
   デフォルトで、「*マネジメント > システム設定 > 組織*」タブの設定が使用されます。

3. **「*エンドポイントプロテクションのアクティベート*」をクリックします。**
   トグルスイッチが緑色になり、エンドポイントプロテクションが有効になります。

   設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

次に、「*エージェントの導入*」ページで、監視するコンピュータに、エンドポイントプロテクションのインストールパッケージをインストールして続行します。

注 – エンドポイントプロテクションを使用する際、「*Webプロテクション > Web フィルタリング > 詳細*」タブの「*Web キャッシング*」にある「*ソフォスエンドポイントのキャッシュを施行*」機能を有効化することを推奨します。これによって、エンドポイントがインターネット経由でアップデートサーバからデータをダウンロードする際、アップリンクが飽和することを阻止できます。

注 – Web フィルタが有効で、透過モードで稼働している場合、エンドポイントがエンドポイントプロテクションを正常に利用できるようにするには、追加の設定が必要になります。エンドポイントプロテクションを有効にすると、UTM によって、*Sophos LiveConnect* という名称の DNS グループが自動的に作成されます。この DNS グループを、「*Web プロテクション > Web フィルタリング > 詳細*」タブにある透過モードスキップリストの「*スキップする宛先ホスト/ネット*」ボックスに追加します。

エンドポイントプロテクションを無効にするには、次の手順に従います:

1. **「*グローバル*」タブで、エンドポイントプロテクションを無効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、2つのオプションが利用可能となります。

2. **エンドポイントのデータを削除するか否かを選択します。**
   全データを保持: 一時的にエンドポイントプロテクションを無効にするには、このオプションを選択します。エンドポイントの設定は保存されます。この機能を再度有効化した際、前回インストールされたエンドポイントは自動的に接続され、定義されていたポリシーが利用されます。

   全データを削除:すべてのエンドポイントの設定を初期状態にリセットするには、このオプションを選択します。エンドポイントの全てのコネクションとポリシー設定が削除されます。この機能を再度有効化した際、エンドポイントが新しい登録データを取得するため、インストレーションパッケージがエンドポイントへ展開されます 。「*コンピュータの管理 > 詳細*」を参照下さい。

3. **「*エンドポイントプロテクションの無効化*」をクリックします。**

トグルスイッチが灰色になり、エンドポイントプロテクションが無効になります。

11.1.2 エージェントの導入

「*エンドポイントプロテクション > コンピュータ管理 > エージェントの導入*」タブでは、エンドポイントプロテクションによりモニタリングする個々のコンピュータ用のインストールファイルを導入できます。

インストールパッケージには 2種類ありますが、提供されるソフトウェアは同じです。各パッケージとも、導入やインストールに関して、それぞれ異なった利点があります。

- **スリムインストールパッケージ:**サイズの小さいパッケージ(12MB)で、容易にメールで提供できます。このパッケージに含まれていないデータは、インストール時にダウンロードされます。

- **フルインストールパッケージ**:完全なインストールデータを含むパッケージ（約 90MB）で、インストール時にダウンロードが必要なデータは最小限に抑えられています。

いずれのパッケージを使用する場合でも、エンドポイントを保護するソフトウェアをエンドポイントに導入する方法には、次の 2とおりあります。

- 「*スリムインストーラのダウンロード*」ボタンや「*フルインストーラのダウンロード*」ボタンをクリックして、インストールパッケージをダウンロードして保存します。その後、エンドポイントユーザに、パッケージへのアクセスを提供します。
- 灰色のボックスに表示されている URL をコピーして、エンドポイントユーザに送信します。エンドポイントユーザはこの URL を使用して、各自インストールパッケージをダウンロードし、インストールします。

注 – インストールパッケージの名前は変更しないでください。インストール時に LiveConnect は、このパッケージ名とUTM の現在登録されているデータを比較します。情報が一致しない場合、インストールは中止されます。

エンドポイントへのインストール後、各コンピュータは、「*コンピュータの管理*」タブに表示されます。さらに、「*詳細*」タブで指定したコンピュータグループに自動的に割り当てられます。

注 –「*詳細*」タブの「*登録トークンのリセット*」ボタンを使用してインストールパッケージを無効にすることができます。

11.1.3 コンピュータの管理

「*エンドポイントプロテクション > コンピュータ管理 > コンピュータ管理*」タブでは、UTMのエンドポイントプロテクションがインストールされているコンピュータの概要を表示することができます。コンピュータはリストに自動的に追加されます。コンピューターをグループに追加すること、追加の情報を加えること、タンパープロテクション設定を修正すること、コンピューターをリストから削除することができます。

リストされているコンピュータのデータを編集するには、次の手順に従います。

1. **各エントリの「編集」ボタンをクリックします。**
   「*コンピュータの編集*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   コンピュータグループ:コンピュータを割り当てるコンピュータグループを選択します。コンピューターはアサインされたグループのプロテクション設定を受け取ります。

タイプ:コンピュータタイプ(デスクトップ、モバイル PC、サーバなど)を選択します。タイプによりリストをフィルタすることができます。

タンパープロテクション:有効化すると、コンピュータの保護設定をローカル変更するにはパスワードが必要となります。このパスワードは、「*詳細*」タブで定義します。無効にすると、エンドポイントユーザはパスワードがなくてもプロテクション設定を変更できます。初期状態では、この設定はコンピューターが所属しているグループと同一となります。

インベントリ #(任意):コンピュータのインベントリ番号を入力します。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   設定が保存されます。

コンピュータを一覧から削除するには、「削除」ボタンをクリックします。

注 – コンピュータをリストから削除すると、UTMエンドポイントプロテクションによりコンピュータが保護されなくなります。しかしながら、インストールされたエンドポイントソフトウエアは自動的にアンインストールされませんし、直近のポリシーは有効なままとなります。

11.1.4 グループ管理

「*エンドポイントプロテクション > コンピュータ管理 > グループ管理*」タブでは、保護されたコンピュータをグループ化し、そのグループに対してエンドポイントプロテクション設定を定義することができます。グループに属するすべてのコンピュータには、同じアンチウイルスポリシーとデバイスポリシーが適用されます。

注 – すべてのコンピュータは一つのグループに所属します。最初は、すべてのコンピュータがデフォルトグループに属します。グループの追加後、「*詳細*」タブでデフォルトとなるグループ、つまり新しくインストールしたコンピュータを自動的に割り当てるグループを定義できます。

コンピュータグループを作成するには、次の手順に従います。

1. **「*コンピュータグループの追加*」をクリックします。**
   「*コンピュータグループの追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このグループを説明する名前を入力します。

ウイルス対策ポリシー:グループに適用するウイルス対策ポリシーを選択します。ポリシーは、「*アンチウイルス > ポリシー*」タブで定義します。「*アンチウイルス > 除外*」タブでこのポリシーからの除外をグループごとに定義できます。

デバイスポリシー:グループに適用するデバイスポリシーを選択します。ポリシーは、「*デバイスコントロール > ポリシー*」タブで定義します。「*デバイスコントロール > 除外*」タブでポリシーからの除外をグループごとに定義できます。

タンパープロテクション:有効化すると、各エンドポイントの保護設定をローカル変更するにはパスワードが必要となります。このパスワードは、「*詳細*」タブで定義します。無効にすると、エンドポイントユーザはパスワードがなくてもプロテクション設定を変更できます。「*コンピュータ管理*」タブでは、個々のコンピュータに異なる設定を適用できます。

Web コントロール:有効化すると、このグループに属するエンドポイントが Sophos UTM ネットワークに接続していない場合でも、Web フィルタリングポリシーを適用して、レポートを送信するようにできます。エンドポイント Web コントロールを有効にするには、「*エンドポイントプロテクション > Web コントロール*」タブを参照してください。

AutoUpdate でプロキシを使用する:有効化すると、このオプションの下にあるフィールドで指定したプロキシの属性が、このグループに属するエンドポイントに送信されます。エンドポイントは、このプロキシデータを使用してインターネットに接続します。

注 – データは誤りのないように入力してください。エンドポイントは、誤ったプロキシデータを受信すると、インターネットや UTM に接続できなくなります。この場合、影響を受けた各エンドポイントで、設定を手動変更する必要があります。

アドレス:プロキシの IP アドレスを入力します。

ポート:プロキシのポート番号を入力します。

ユーザ:必要に応じて、プロキシのユーザ名を入力します。

パスワード:必要に応じて、プロキシのパスワードを入力します。

コンピュータ:グループに含めるコンピュータを追加します。

コメント(任意):説明などの情報を追加します。

3. **「保存」をクリックします。**
   グループが作成され、「*グループの管理*」リストに表示されます。設定の変更後にすべてのコンピュータが設定されるまで、15分ほどかかる場合があることに注意してください。

グループを編集または削除するには、対応するボタンをクリックします。

11.1.5 詳細

「*エンドポイントプロテクション > コンピュータ管理 > 詳細*」タブでは、次のオプションを設定できます。

タンパープロテクション:タンパープロテクションを有効化すると、エンドポイントの保護設定を変更するには、このパスワードが必要になります。

デフォルトコンピュータグループ:エンドポイントプロテクションのインストール後間もなく、コンピュータを自動的に割り当てるコンピュータグループを選択します。

Sophos LiveConnect – 登録:このセクションには、エンドポイントプロテクションの登録情報が表示されます。このデータは、インストールパッケージを識別するために使用され、さらにサポート目的でも使用されます。

- **登録トークンのリセット**:以前に導入されたインストールパッケージを使ってインストールが行われることを防止するには、このボタンをクリックします。これは、通常、インストールを完了する際に実行します。新しいエンドポイントにインストールする場合は、「*エージェントの導入*」タブで、新しいインストールパッケージを作成してください。

11.2 ウイルス対策

「*エンドポイントプロテクション > ウイルス対策*」ページでは、エンドポイントプロテクション機能のウイルス対策設定を定義できます。ウイルス対策ポリシー(つまり、一連のウイルス対策設定)を作成し、後で、これをコンピュータグループに適用し、エンドポイントプロテクションでモニタリングすることができます。さらに、特定のコンピュータグループに適用するウイルス対策機能の例外を定義することもできます。

11.2.1 ポリシー

「*エンドポイントプロテクション > アンチウイルス > ポリシー*」タブでは、一連のアンチウイルス設定を管理できます。その後ポリシーをコンピュータグループに適用してエンドポイントプロテクションでモニタリングすることができます。

デフォルトでは、*基本プロテクション*アンチウイルスポリシーが使用できます。これを使用すると、脅威に対するコンピュータの防護と全般的なシステムパフォーマンスの間で最も良好なバランスが得られます。このポリシーは変更できません。

アンチウイルスポリシーを追加するには、次の手順に従います。

1. **「*ポリシーの追加*」ボタンをクリックします。**
   「*ポリシーの追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このポリシーを説明する名前を入力します。

   オンアクセススキャン:これを有効にすると、ファイルをコピーまたは移動したり、開くたびに、ファイルがスキャンされ、コンピュータに脅威を及ぼさない場合、または使用が許可されている場合のみにアクセスが許可されます。

   - **PUA をスキャン:**これを有効にすると、オンアクセススキャンの一環で PUA（不要と思われるアプリケーション）がないかチェックされます。

   自動クリーンアップ:これを有効にすると、ウイルスまたはスパイウェアを含むアイテムはクリーンアップされ、マルウェアそのものは削除され、感染したアイテムは駆除されます。ウイルススキャナは以前に含まれていたファイルの内容が破損しているかどうかを把握できないため、ウイルス駆除を行ったこれらのファイルは、永久的に破損しているものとみなす必要があります。

   Sophos Live Protection:エンドポイントコンピュータのウイルス対策スキャンでファイルが疑わしいと判断されても、コンピュータに保存されている Sophos 脅威 ID（IDE）ファイルを基にして、それがクリーンなファイルか悪意のあるファイルかを特定できない場合、詳細な分析を行うために、特定のファイルデータ（チェックサムやその他の属性など）が Sophos に送信されます。

   クラウド内チェックは、SophosLabs データベースで疑わしいファイルの即時ルックアップを実施します。ファイルをクリーンなファイルまたは悪意のあるファイルと特定した場合は、コンピュータにその判定が送り返され、ファイルのステータスが自動的に更新されます。

   - **サンプルファイルの送信:**ファイルが疑わしいとみなされても、ファイルのデータだけでは、確信を持って悪意のあるファイルと特定できない場合、サンプルファイルのリクエストを Sophos に許可することができます。このオプションを有効にすると、既にそのファイルのサンプルが Sophos にない場合、ファイルが自動的に送信されます。サンプルファイルを送信することで、Sophosでは誤検出を行うことなく、マルウェア検出を継続的に改善することができます。

   疑わしい動作検出 (HIPS):これを有効にすると、レジストリへの疑わしい書き込み、ファイルのコピーアクション、バッファオーバーフロー技術などのアクティブなマルウェアの兆候がないか、すべてのシステムプロセスがモニタリングされます。疑わしいプロセスはブロックされます。

Web プロテクション:これを有効にすると、感染 Web サイトの Sophos オンラインデータベースで、各 Web サイトの URL が参照されます。

- **悪意のあるサイトブロック:**これを有効にすると、悪意のあるコンテンツのサイトはブロックされます。
- **ダウンロードスキャン:**これを有効にすると、ウイルス対策スキャンによりダウンロード中のデータがスキャンされ、悪意のあるコンテンツが含まれる場合はブロックされます。

スケジュールスキャン:これを有効にすると、指定した日時にスキャンが実行されます。

- **ルートキットスキャン:**これを有効にすると、スケジュールスキャンを実行するたびに、コンピュータのルートキット検索が実行されます。
- **低い優先度での検索:**これを有効にすると、オンデマンド検索は、低い優先度で実行されます。なお、これは Windows Vista SP 2 以降のみで指定できます。
- **時間帯:**エンドポイントのタイムゾーンを考慮して、スキャンを実施する時間帯を選択します。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しいポリシーがアンチウイルスポリシーリストに表示されます。設定の変更後にすべてのコンピュータが設定されるまで、15分ほどかかる場合があることに注意してください。

ポリシーを編集または削除するには、対応するボタンをクリックします。

11.2.2 除外

「*エンドポイントプロテクション > ウイルス対策 > 除外*」タブで、エンドポイントプロテクションのウイルス対策設定からの除外をコンピュータグループごとに定義できます。除外を設定すると、アンチウイルスポリシー設定のために行われるスキャンからアイテムが除外されます。

除外を追加するには、次の手順に従います。

1. **「*除外*」タブで、「*新規除外リスト*」をクリックします。**
   「*除外リストを作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   タイプ:オンアクセススキャンおよびオンデマンドスキャンから除外するアイテムのタイプを選択します。

- **アドウェアとPUA:**これを選択すると、スキャンとブロックから特定のソフトウェアまたはPUA(不要と思われるアプリケーション)を除外できます。アドウェアは、ユーザの生産性やシステム効率に影響を与える可能性のある広告(ポップアップメッセージなど)を表示します。PUAは悪意あるソフトウェアではないものの、一般的にビジネスネットワークに不適切とみなされています。「*ファイル名*」フィールドに、`example.stuff`など、アドウェアやPUAの名前を追加します。
- **スキャン除外:**これを選択すると、ファイル、フォルダ、またはネットワークドライブをウイルス対策スキャンから除外できます。「*ファイル/パス*」フィールドに、`C:\Documents\` や `\\Server\Users\Documents\CV.doc` など、ファイル、フォルダ、またはネットワークドライブを入力します。
- **スキャン対象拡張子:**これを選択すると、ウイルス対策スキャンから特定の拡張子のファイルを除外できます。「*拡張子*」フィールドに、`html`など、拡張子を入力します。
- **バッファオーバーフロー:**これを選択すると、バッファオーバーフロー技術を使用するアプリケーションが動作モニタリングでブロックされるのを防止することができます。必要に応じて、「*ファイル名*」フィールドにアプリケーションファイル名を入力し、「*アップロード*」フィールドでそのファイルをアップロードしてください。
- **疑わしいファイル:**これを選択すると、疑わしいファイルがウイルス対策スキャンでブロックされるのを防止することができます。「*アップロード*」フィールドでファイルをアップロードします。UTMは、ファイルのMD5チェックサムを生成します。アップロードしたファイルの名前は、自動的に「*ファイル名*」フィールドで使用されます。このファイル名は変更することもできます。ここで指定したファイル名と保存されたMD5チェックサムのあるファイルがクライアントで検出された場合、それはウイルス対策スキャンによってブロックされません。
- **疑わしい動作:**これを選択すると、ファイルが疑わしい動作検知でブロックされるのを防ぐことができます。必要に応じて、「*ファイル名*」フィールドにファイル名を入力し、「*アップロード*」フィールドでそのファイルをアップロードしてください。
- **Webサイト:**これを選択すると、[*Webフォーマット*」フィールドで指定したプロパティのWebサイトは、ウイルス対策スキャンされません。
  Webフォーマット:閲覧を許可するWebサイトのサーバを指定します。
  - **ドメイン名:**許可するドメインの名前を「*Webサイト*」フィールドに入力します。
  - **IPアドレスとサブネットマスク:**許可するコンピュータのIPv4アドレスとネットマスクを入力します。
  - **IPアドレス:**許可するコンピュータのIPv4アドレスを入力します。

アップロード（*バッファオーバーフロー*、**疑わしいファイル**、および*疑わしい動作*タイプのみ）：ウイルス対策スキャンから除外するファイルをアップロードします。

コンピュータグループ：除外対象のコンピュータグループを追加または選択します。

コメント（任意）：説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しい除外が「*除外*」リストに表示されます。

除外ルールを編集または削除するには、対応するボタンをクリックします。

11.3 デバイスコントロール

「*エンドポイントプロテクション > デバイスコントロール*」ページでは、エンドポイントプロテクションを使ってモニタリングしているコンピュータに接続されたデバイスを管理できます。デバイスポリシーで、ポリシーが適用されたコンピュータグループに対して、許可またはブロックするデバイスのタイプを定義します。デバイスを検出すると、エンドポイントプロテクションは各コンピュータのコンピュータグループに適用されているデバイスポリシーに従って、デバイスが許可されているかどうかをチェックします。デバイスポリシーでブロックまたは制限が指定されている場合は、デバイスが「*除外*」タブに表示され、ここでデバイスの除外を追加することができます。

11.3.1 ポリシー

「*エンドポイントプロテクション > デバイスコントロール > ポリシー*」タブでは、一連のデバイスコントロール設定を管理できます。その後これをコンピュータグループに適用してエンドポイントプロテクションでモニタリングすることができます。これらの設定は、デバイスポリシーと呼ばれています。

デフォルトで、2種類のデバイスポリシーがあります。「*Blocked All*」（すべてをブロック）はあらゆるタイプのデバイスの使用を禁止し、「*Full Access*」（フルアクセス）は、すべてのデバイスに対してすべての権限を許可します。これらのポリシーは変更できません。

新しいポリシーを追加するには、以下の手順に従います。

1. **「*ポリシーの追加*」ボタンをクリックします。**
   「*ポリシーの追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前：このポリシーを説明する名前を入力します。

ストレージ機器:各種ストレージデバイスに対して、「*許可*」または「*ブロック*」を指定できます。該当する場合は、「*読取専用*」エントリも選択できます。

ネットワーク機器:モデムおよびワイヤレスネットワークに対しては、「*許可*」、「*ブリッジをブロック*」、「*ブロック*」のいずれかを指定できます。

近距離通信機器: Bluetooth や赤外線デバイスに対しては、「*許可*」または「*ブロック*」を指定できます。

3. **コメント**(任意):説明などの情報を追加します。
4. **「*保存*」をクリックします。**
   新しいポリシーがデバイスコントロールリストに表示されます。これをコンピュータグループに適用することができます。設定の変更後にすべてのコンピュータが設定されるまで、15分ほどかかる場合があることに注意してください。

ポリシーを編集または削除するには、対応するボタンをクリックします。

11.3.2 除外

「*エンドポイントプロテクション > デバイスコントロール > 除外*」タブでは、デバイスに対する保護の例外を指定できます。機器を指定することで、コンピュータグループに適用されたデバイスポリシーで禁止されている設定が許可されます。例外はコンピュータグループに対して指定されるため、選択したグループ内のコンピュータすべてに適用されます。

「*機器*」リストには、デバイスコントロール ポリシーによりブロックまたはアクセス制限が行われているデバイスが自動的に表示されます。複数のフロッピードライブを接続している場合、各ドライブを区別できないため1つのみが表示され、これがすべてのフロッピードライブのプレースホルダとして機能します。

デバイスに対する機器を追加するには、次の手順に従います。

1. **デバイスの「*編集*」ボタンをクリックします。**
   「*デバイスの編集*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   許可:このデバイスを許可するコンピュータグループを追加します。

   読込専用/ブリッジ:読み取り専用モード(ストレージデバイスに適用)またはブリッジモード(ネットワークデバイスに適用)でこのデバイスを許可するコンピュータグループを追加します。

すべてに適用:これを選択すると、デバイス ID が同じデバイスすべてに現在の設定が適用されます。これは、同じタイプの複数の USB メモリに、一般的な例外を適用する場合などに便利です。

モード:このオプションは、「*すべてに適用*」チェックボックスを選択から外した場合のみに使用できます。この場合、一般的な機器が指定されている他のデバイスに対する処理を指定する必要があります。該当するデバイスで、一般的な例外を引き続き指定するには、「*他のデバイスでは保持*」を選択します。一般的な例外を削除するには、「*他のデバイスでは削除*」をクリックします。

ヒント – 一般的な機器に関する詳細および例は、以下の「デバイスの一般的な機器について」を参照してください。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**

   編集したデバイスに対して、コンピュータグループおよび指定されている例外が表示されます。

ヒント – 「*機器*」リストに表示されたデバイスは、「*削除*」ボタンを使用して削除しない限り、表示されたままになります。通常、対応するハードウェアデバイスが削除された(例: 光学デバイスが存在しなくなった)、またはデバイスポリシーを変更した(例: ワイヤレス ネットワーク アダプタが一般に許可されるようになった)場合などに、デバイスのエントリを削除します。使用中のデバイスのエントリを削除すると、確認メッセージが表示されるので、「*OK*」をクリックしてください。その後、デバイスは、リストから削除されます。このデバイスに対して機器が指定されていた場合、例外は自動的に無効になり、現在のデバイスポリシーがデバイスに適用されるようになります。

デバイスの一般的な機器について

デバイスの一般的な機器は、デバイス ID が同じデバイスすべてに自動的に適用される例外です。

一般的な機器を作成する

1. 一般的な機器が指定されていない(つまり、「*すべてに適用*」チェックボックスが選択から外されている)デバイスの「*編集*」ボタンをクリックします。
2. 機器を設定して、「*すべてに適用*」チェックボックスを選択します。

3. 機器を保存します。
この例外は、デバイス ID が同じデバイスすべてに適用されます。

一般的な機器からデバイスを除外する

1. 既存の一般的な例外から除外するデバイスの「*編集*」ボタンをクリックします。
2. 個別の例外を設定して、「*すべてに適用*」チェックボックスを選択から外します。
3. 「*モード*」ドロップダウンリストで、「*他のデバイスでは保持*」を選択します。
4. 例外を保存します。
編集したデバイスには個別の機器が指定されるようになりましたが、他のデバイスでは一般的な機器が保持されています。

一般的な機器のあるデバイスすべての設定を変更する

1. 一般的な機器が指定されているいずれかのデバイスの「*編集*」ボタンをクリックします。
2. 機器を設定し、「*すべてに適用*」チェックボックスは選択したままにします。
3. 機器を保存します。
「*すべてに適用*」チェックボックスが選択されているデバイスすべてに対する設定が変更されます。

一般的な機器を削除する

1. 一般的な例外が指定されているいずれかのデバイスの「*編集*」ボタンをクリックします。
2. 「*すべてに適用*」チェックボックスを選択から外します。
3. 「*モード*」ドロップダウンリストで、「*他のデバイスでは削除*」を選択します。
4. 機器を保存します。
「*すべてに適用*」チェックボックスが選択されているデバイスすべてに対する例外が削除されます。機器（個別の機器）が指定されているのは、編集したデバイスのみになりました。

11.4 Webコントロール

企業ネットワーク内からインターネットにアクセスする場合、Sophos UTM によってシステムのセキュリティと生産性の保護が提供されますが、エンドポイント Web コントロール機能は、これをユーザのマシンに拡張します。これによって、企業ネットワーク外のエンドポイントコンピュータや、移動先で使用するモバイル PC に、保護・コントロール・レポート機能を提供することができます。有効化されると、「*Webプロテクション > Web フィルタリング*」および「*Webプロテクション > Web フィルタリングプロファイル > プロキシプロファイル*」で定義したポリシーは、コンピュータが UTM ネットワーク上にない

場合でも、エンドポイント Web コントロール機能によって施行されます。Sophos UTMおよび Sophos エンドポイントは、LiveConnect を通じで通信し、Sophos UTM と移動先の Sophos エンドポイントをクラウド経由でシームレスに接続することで、ポリシーやレポートの更新をリアルタイムで実現します。たとえば、自宅やネットカフェで使用するモバイル PC にも Web コントロール ポリシーを施行することが可能で、Sophos UTM は、移動先のモバイル PC からログ情報を受信します。

11.4.1 グローバル

「*エンドポイントプロテクション > Web コントロール > グローバル*」タブで、エンドポイント Web コントロールを有効または無効にできます。エンドポイント Web コントロールのフィルタリングポリシーを設定するには、該当するグループの Web コントロールを、「*エンドポイントプロテクション > コンピュータ管理*」ページで有効化し、「*Webプロテクション > Web フィルタリング > プロキシプロファイル*」タブのプロキシプロファイルで、そのグループを参照する必要があります。

11.4.2 詳細

「*エンドポイントプロテクション > Web コントロール > 詳細*」タブで、「*ゲートウェイとエンドポイントの両方でトラフィックをスキャンする*」を選択できます。デフォルトで Sophos UTM は、Web コントロールが有効化されているエンドポイントの Web トラフィックをスキャンしません。このオプションを有効化すると、エンドポイントと Sophos UTM の両方によって Web トラフィックがフィルタリングされます。新たなレイヤーのセキュリティを提供するためには、「*Webプロテクション > Web フィルタリング > ウイルス対策/マルウェア対策*」で「*デュアルスキャン(セキュリティ最適化)*」を指定してください。または、「*管理 > システム設定 > スキャン設定*」タブで、別の検索エンジンを選択してください。いずれの場合でも、エンドポイントで使用している検索エンジンとは別の検索エンジンが Sophos UTM で使用されるので、セキュリティが向上します。

11.4.3 対応していない機能

Web コントロール機能をエンドポイントに拡張するメリットは多数ありますが、Sophos UTM ネットワークのみで使用できる機能もあります。Sophos UTM では対応しているが、エンドポイント Web コントロールでは対応していない機能は次のとおりです。

- **HTTPS (SSL)トラフィックをスキャン:**HTTPS トラフィックをエンドポイントでスキャンすることはできません。エンドポイントがプロキシ経由で UTM を使用している場合、この機能が有効化されていると、トラフィックは UTM によってスキャンされます。

- **認証モード:**エンドポイントは、現在ログインしているユーザ(SSO)を常に使用します。エンドポイントは認証を実行できません。エンドポイントを移動先で使用している場合、UTM に接続して認証することはできません。
- **ウイルス対策/マルウェア対策:**Sophosエンドポイントのウイルス対策は、「*エンドポイントプロテクション > ウイルス対策*」ページで設定します。Web Protection(ダウンロードスキャン)を有効にしている場合、すべての Web コンテンツに対して、常にウイルスのシングスキャンを実行します。デュアルスキャンおよび最大スキャンサイズには対応していません。
- **アクティブコンテンツ除去**
- **YouTube for Schools**
- **ストリーミング設定:**Sophos エンドポイントは、ストリーミングコンテンツに対するウイルス検索を常に実行します。
- **スキャンできないファイル、暗号化されたファイルのブロック**
- **ダウンロードサイズでブロック**
- **許可するターゲットサービス:**この機能は、Sophos UTM のみで使用できます。
- **Web キャッシング:**この機能は、Sophos UTM のみで使用できます。

12 ワイヤレスプロテクション

「*ワイヤレスプロテクション*」メニューを使用して、Sophos UTMのワイヤレスアクセスポイント、対応するワイヤレスネットワーク、ワイヤレスアクセスを利用するクライアントを設定および管理することができます。アクセスポイントはUTM上で自動的に設定されるため、個別に設定する必要はありません。アクセスポイントの設定およびステータス情報を交換するために使用される、UTMとアクセスポイントの間の通信は、AESを使用して暗号化されます。

重要 – アクセスポイントが激しく点滅している場合は、電源を切断しないでください。激しい点滅は、ファームウェアフラッシュが現在行われていることを意味します。ファームウェアフラッシュは、ワイヤレスプロテクション更新に伴うUTMシステム更新の後などに実行されます。

この章では、次のトピックについて説明します。

- グローバル設定
- ワイヤレスネットワーク
- メッシュネットワーク
- アクセスポイント
- ワイヤレスクライアント
- ホットスポット

ワイヤレスプロテクションの概要ページは、接続されたアクセスポイント、そのステータス、接続されたクライアント、ワイヤレスネットワーク、メッシュネットワーク、およびメッシュのピアリンクに関する基本情報を示します。

「*接続中*」セクションでは、エントリをSSIDまたはアクセスポイント別に並べ替えることができます。各エントリは、左にあるアイコンをクリックして展開したり折りたたみ表示にしたりできます。

ライブログ

「*ワイヤレスプロテクションライブログを開く*」ボタンをクリックすると、アクセスポイントおよび接続を試行するクライアントに関する詳細な接続およびデバッグ情報が表示されます。

12.1 グローバル設定

「*ワイヤレスプロテクション > グローバル設定*」ページでは、ワイヤレスプロテクションの有効化、ワイヤレスプロテクション用のネットワークインタフェースの設定、および WPA/WPA2 エンタープライズ認証の設定が可能です。

12.1.1 グローバル設定

「*ワイヤレスプロテクション > グローバル設定 > グローバル設定*」タブで、ワイヤレスプロテクションを有効または無効にできます。

ワイヤレスプロテクションを有効にするには、次の手順に従います。

1. **「*グローバル設定*」タブで、ワイヤレスプロテクションを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*アクセスコントロール*」エリアが編集可能になります。

   ワイヤレスプロテクションを初めて有効にする際は、「*初期セットアップ*」セクションが表示されます。ここには作成される設定が表示されます。WPA2 個人暗号化を DHCP 用ワイヤレス クライアントで使用する個別のワイヤレス「ゲスト」ネットワーク。このクライアントは、UTM および *Web サーフィン*サービスで DNS を使用することが許可されます。事前共有鍵は自動生成され、このセクションのみに表示されます。初期設定はテンプレートとして機能します。いつでも「*ワイヤレスプロテクション > ワイヤレスネットワーク*」ページで設定を編集することができます。

   自動設定のスキップ:また、このオプションを選択して、初期セットアップをスキップすることもできます。この場合、ワイヤレス設定を手動で行う必要があります。

2. **アクセスポイント用のネットワークインタフェースを選択します。**
   アクセスポイントをプラグインする設定済みインタフェースを選択するには、「*許可されるインタフェース*」セクションのフォルダアイコンをクリックします。DHCP サーバがこのインタフェースに関連付けられていることを確認してください。

3. **「*適用*」をクリックします。**

   設定が保存されます。トグルスイッチが緑色になり、ワイヤレスプロテクションが有効になります。

設定されたネットワークインタフェースにアクセスポイントをプラグインして、続行することができます。自動設定のスキップを選択した場合は、「*ワイヤレスネットワーク*」ページで設定を続けます。

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

アクセスポイントをプラグインするとすぐに、アクセスポイントはシステムに自動的に接続します。新たに接続された未設定のアクセスポイントは、「*アクセスポイント > 概要*」ページに「*保留中のアクセスポイント*」としてリストされます。

12.1.2 詳細

「*ワイヤレスプロテクション > グローバル設定 > 詳細*」タブでは、WPA/WPA2 エンタープライズ認証を使用するようにアクセスポイントを設定することができます。

エンタープライズ認証には、RADIUS サーバのいくつかの情報を入力する必要があります。AP は認証のために RADIUS サーバと通信せず、UTMとだけ通信します。UTM と AP の間の RADIUS 通信にはポート `414` が使用されます。

WPA/WPA2 エンタープライズ認証を使用にするには、次の設定を行います。

RADIUS サーバ:クライアントが自己認証を行うサーバを選択または作成します (Active Directory サーバなど)。

RADIUS ポート (オプション):デフォルトでは、RADIUS ポート 1812 が選択されています。必要であれば、ポートを変更できます。

RADIUS シークレット:アクセスポイントが RADIUS サーバと通信するために必要な RADIUS パスフレーズを入力します。

シークレットの確認:セキュリティ上の理由で、ここで RADIUS パスフレーズをもう一度入力します。

設定を保存するには「*適用*」をクリックします。

12.2 ワイヤレスネットワーク

「*ワイヤレスプロテクション > ワイヤレスネットワーク*」ページでは、ワイヤレスネットワークを定義できます (SSID や 暗号化方式など)。さらに、ワイヤレスネットワークに個別の IP アドレス範囲が必要か、アクセスポイントの LAN に対するブリッジングが必要かを定義することができます。

新しいワイヤレスネットワークを作成するには、次の手順に従います。

1. **「*ワイヤレスネットワーク*」ページで「*ワイヤレスネットワークの追加*」をクリックします。**
「*ワイヤレスネットワークの追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
ネットワーク名:ネットワークを説明する名前を入力してください。

ネットワーク SSID:ワイヤレスネットワークの識別のためにクライアントに表示される、ネットワークのサービスセット識別子(SSID)を入力します。SSID は、1～32 文字の ASCII 印字可能文字[1]で構成します。コンマは使用できず、先頭または末尾をスペースにすることはできません。

暗号化モード:ドロップダウンリストから暗号化モードを選択します。デフォルトは *WPA 2 パーソナル* です。できる限り、*WPA* よりも *WPA2*を使用することをお勧めします。セキュリティ上の理由から、ワイヤレスネットワークを使用しているクライアントの中に、WEP 以外の方法をサポートしないクライアントがいなければ、WEP を使用しないことを推奨します。エンタープライズ認証方式を使用する場合、「*グローバル設定 > 詳細*」タブで RADIUS サーバも設定する必要があります。RADIUS サーバ の NAS ID として、ワイヤレスネットワーク名を入力します。

パスフレーズ/PSK:*WPA/WPA2 パーソナル* 暗号化モードのみで使用できます。許可されないアクセスからワイヤレスネットワークを保護するパスフレーズを入力し、次のフィールドに再入力してください。パスフレーズには、8～63文字の ASCII 印字可能文字を使用します。

128 ビット WEP キー:*WEP* 暗号化モードのみで使用できます。ここで、26文字ちょうどの 16進文字から成る WEP キーを入力します。

クライアントトラフィック:ワイヤレスネットワークをローカルネットワークに統合する方法を選択します。

- **別ゾーン**(デフォルト):ワイヤレスネットワークは、独自の IP アドレス範囲を持つ独立したネットワークとして処理されます。このオプションを使用する場合、ワイヤレスネットワークを追加した後に、次のセクション(分離ゾーンネットワークの次のステップ)の手順に従ってセットアップを継続する必要があります。

  注 – 既存の *別ゾーンネットワーク*を「*AP LAN へのブリッジ*」または「*VLAN へのブリッジ*」に切り替えると、UTM上の設定済み WLAN インタフェースは *未割り当て*

[1] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters

(unassigned) になります。ただし、編集して再有効化することにより、新しいハードウェアインタフェースをインタフェースオブジェクトに割り当てることができます。

- **APのLANにブリッジ:**ワイヤレスネットワークをアクセスポイントのネットワークにブリッジングすることができます。つまり、ワイヤレスクライアントは同じIP アドレス範囲を共有します。

  注 – VLAN が有効な場合、ワイヤレスクライアントはアクセスポイントの VLAN ネットワークにブリッジングされます。

- **VLAN にブリッジ:**このワイヤレスネットワークのトラフィックを任意の VLAN にブリッジングさせることができます。これは、ワイヤレスクライアントから独立した共通ネットワーク内にアクセスポイントを含めたい場合に便利です。
  VLAN ID にブリッジ:ワイヤレスクライアントが含まれるネットワークの VLAN ID を入力します。

  クライアント VLAN ID (*エンタープライズ*暗号化モードのみで使用可能):VLAN ID を定義する方法を選択します。

  - **スタティック:**「*VLAN ID にブリッジ*」フィールドに定義された VLAN ID を使用します。
  - **RADIUS とスタティック:**RADIUS サーバが提供する VLAN ID を使用します。ユーザがいずれかのワイヤレスネットワークに接続し、RADIUS サーバで認証を行うと、RADIUS サーバはこのユーザに対して使用すべき VLAN ID をアクセスポイントに知らせます。したがって、複数のワイヤレスネットワークを使用する際に、どのユーザがどの内部ネットワークにアクセスできるのかをユーザごとに定義することができます。ユーザに VLAN ID 属性が割り当てられていない場合、「*VLAN ID へのブリッジ*」フィールドで定義された VLAN ID が使用されます。

コメント (任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   アルゴリズム (WPA/WPA2 暗号化モードでのみ使用可能):暗号化アルゴリズムを *AES* または *TKIP & AES* から選択します。セキュリティ上の理由から、*AES* を使用することをお勧めします。

周波数帯:このワイヤレスネットワークに割り当てられたアクセスポイントは選択した周波数帯で送信を行います。5 GHz帯は、通常パフォーマンスが高い一方で、レイテンシが低く、一般的に干渉も少なくなっています。したがって、VoIP 通信などに優先使用するようにしてください。AP 50 のみで 5 GHz帯での送信が可能です。

タイムベースアクセス:タイムスケジュールに応じてワイヤレスネットワークを自動的に有効/無効にするには、このオプションを選択します。

有効な時間帯の選択:ワイヤレスネットワークを有効にする時間を定義した時間帯定義を選択します。「+」アイコンをクリックして新しい時間帯定義を追加できます。

クライアントアイソレーション:ネットワーク内のクライアントは通常、互いに通信できます。ゲストネットワーク内などでこれを禁止したい場合、ドロップダウンリストで「*有効*」を選択します。

SSID 非表示:SSID を非表示にする場合に選択します。この場合、ドロップダウンリストから「*はい*」を選択します。これはセキュリティ機能ではありません。

MAC フィルタリングタイプ:このワイヤレスネットワークへの接続が許可される MAC アドレスを制限するには、「*ブラックリスト*」または「*ホワイトリスト*」を選択します。*ブラックリスト*を使用する場合、以下の MAC アドレスリストで指定したものを除く、すべての MAC アドレスが許可されます。*ホワイトリスト*を使用する場合、以下の MAC アドレスリストで指定したものを除く、すべての MAC アドレスがブロックされます。

MAC アドレス:ワイヤレスネットワークへのアクセスを制限するために使用する MAC アドレスのリスト。MAC アドレスのリストは、「*定義とユーザ > ネットワーク定義 > MAC アドレス定義*」タブで作成できます。

4. **「*保存*」をクリックします。**
   設定が保存されます。ワイヤレスネットワークが「*ワイヤレスネットワーク*」リストに表示されます。

別ゾーンネットワークの次のステップ

「*別ゾーン*」オプションを指定してワイヤレスネットワークを作成した場合、*wlan0* のように、対応する新しい仮想ハードウェアインタフェースが自動的に作成されます。このワイヤレスネットワークを使用するためには、更なる手動設定が必要になります。次の手順で実行します。

1. **新しいネットワークインタフェースを設定します。**
   「*インタフェース & ルーティング > インタフェース > インタフェース*」タブで新しいインタフェースを作成し、ハードウェアとして wlan インタフェース (wlan0 など) を選択します。タイプが「イーサ

ネット」であることを確認し、ワイヤレスネットワークの IP アドレスとネットマスクを指定します。

2. **ワイヤレスクライアントの DHCP を有効にします。**
クライアントがUTMに接続できるようにするためには、クライアントに IP アドレスとデフォルトゲートウェイを割り当てる必要があります。そのため、「*ネットワークサービス > DHCP > サーバ*」タブで、このインタフェースに DHCP サーバをセットアップします。

3. **ワイヤレスクライアントの DNS を有効にします。**
クライアントが DNS 名を解決できるようにするためには、クライアントが DNS サーバにアクセスできるようにする必要があります。「*ネットワークサービス > DNS > グローバル*」タブで、許可ネットワークリストにインタフェースを追加します。

4. **ワイヤレスネットワークをマスクする NAT ルールを作成します。**
その他のネットワークと同様に、ワイヤレスネットワークのアドレスをアップリンクインタフェースのアドレスに変換する必要があります。「*ネットワークプロテクション > NAT > マスカレード*」タブで NAT ルールを作成します。

5. **1つ以上のパケットフィルタルールを作成して、ワイヤレスネットワークとのトラフィックの送受信を許可します。**
その他のネットワークと同様に、1つ以上のパケットフィルタルールを作成して、Web サーフィントラフィックなどのトラフィックがUTMを通過できるようにします。「*ネットワークプロテクション > ファイアウォール > ルール*」タブでパケットフィルタルールを作成します。

12.3 アクセスポイント

「*ワイヤレスプロテクション > アクセスポイント*」ページは、システムで認識されているアクセスポイント（AP）の概要を示します。ここでは、AP の属性の編集、AP の削除またはグループ化、AP または AP グループへのワイヤレスネットワークの割り当てを行うことができます。

注 – ベーシックガードサブスクリプションでは、1つのアクセスポイントのみ UTM にアクセスが可能です。

アクセスポイントのタイプ

現在、Sophosでは、4種類のアクセスポイントを用意しています。

- AP 5: 802.11b/g/n 規格、2.4 GHz 帯
USB コネクターで RED rev2 または rev3 のみに接続が可能です。また、WLAN タイプが「*AP*

LAN にブリッジ」の 1つの SSID をサポートし、最大 7台のワイヤレスクライアントに対応します。

- AP 10：802.11b/g/n規格、2.4 GHz帯
- AP 30：802.11b/g/n規格、2.4 GHz帯
- AP 50：802.11a/b/g/n規格、2.4/5 GHzデュアルバンド/デュアルラジオ
  AP 50 には、使用できるチャネルが異なる 2つのモデルがあります。
  - FCC 規制準拠ドメイン（主に米国）: チャネル 1～11、36、40、44、48
  - ETSI 規制準拠ドメイン（主に欧州）: チャネル 1～13、36、40、44、48

  AP の国設定によって、各地の法律に準拠するために使用できるチャネルが決まりますので、ご注意ください。

参照 – アクセスポイントについての詳細は、Sophos UTMリソースセンターにある「*取扱説明書*」を参照してください。

12.3.1 概要

「*ワイヤレスプロテクション > アクセスポイント > 概要*」ページは、システムで認識されているアクセスポイント（AP）の概要を示します。Sophos UTMは、アクティブ、インアクティブ、保留中の AP を識別します。正規の AP のみがネットワークに接続するようにするために、最初に AP を承認する必要があります。

注 – AP 5を使用する場合は、最初に RED マネジメントを有効にして、RED をセットアップします。その後、RED インタフェースが「*ワイヤレスプロテクション > グローバル設定*」ページの許可インタフェースに追加されていることを確認します。AP 5を RED に接続した後は、AP 5 が「*保留中のアクセスポイント*」セクションに表示されるはずです。

アクセスポイントは「*グループ化*」タブで一時的に無効化できます。APをネットワークから物理的に削除する場合、ここで「*削除*」ボタンをクリックして削除します。AP がネットワークに接続されている限り、削除後も「*保留中*」状態で自動的に再表示されます。

ヒント – このページの各セクションは、セクションヘッダの右にあるアイコンをクリックして、折りたたみ/展開できます。

アクティブなアクセスポイント

ここには、接続されており設定済みで実行中の AP がリストされます。AP を編集するには、「*編集*」ボタンをクリックします(「*アクセスポイントの編集*」を参照)。

インアクティブなアクセスポイント

ここには、過去に設定済みで現在はUTMに接続されていない AP がリストされます。AP がこの状態で 5分間経過した場合、AP のネットワーク接続とシステムの設定を確認してください。ワイヤレスプロテクションサービスを再起動すると、「*最後のアクセス (Last seen)*」タイムスタンプが消去されます。AP を編集するには、「*編集*」ボタンをクリックします(「*アクセスポイントの編集*」を参照)。

保留中のアクセスポイント

ここには、システムに接続されているが未承認の AP がリストされます。AP を承認するには、「*同意*」ボタンをクリックします(「*アクセスポイントの編集*」参照)。

設定の受信後、今承認されたアクセスポイントが、現在アクティブであるか否かに応じて、上のいずれかのセクションに即時に表示されるようになります。

アクセスポイントの編集

1. **各アクセスポイントの「*編集*」または「*承諾*」ボタンをクリックします。**
   「*アクセスポイントの編集*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   ラベル (オプション):ネットワークの AP を簡単に特定するためにラベルを入力します。

   国:AP が設置された国を選択します。

   > **重要 –** 国コードにより、送信に使用できるチャネルが決まります。各地の法律に準拠するために、正しい国を選択してください(「アクセスポイント」の章を参照してください)。

   グループ (オプション):AP をグループ化することができます。以前にグループを作成している場合は、ドロップダウンリストから選択できます。それ以外の場合は、「*新規グループ*」を選択し、「*名前*」テキストボックスにグループ名を入力します。グループ化の設定は「*グループ化*」タブで行います。

3. **「*ワイヤレスネットワーク*」セクションで、次の設定を行います。**
   ワイヤレスネットワークの選択 (グループが 1つも選択されてないか新規グループが選択されている場合):アクセスポイントがブロードキャストするワイヤレスネットワークを選択しま

す。これは、オフィスにのみブロードキャストすべき会社のワイヤレスネットワークや、建物内の公共部分のみでブロードキャストすべきゲストワイヤレスネットワークなどで便利です。リストヘッダのフィルタフィールドを使用して、ワイヤレスネットワークを検索することができます。

注 – アクセスポイントがワイヤレスネットワークにブロードキャストするには、いくつか条件を満たす必要があります。詳細は、「AP へのネットワーク割り当てルール」セクションを参照してください。

4. **必要に応じて、「メッシュネットワーク」セクションで、次の設定を行います**(AP 50 のみ。またメッシュネットワークが「メッシュネットワーク」タブで定義されている場合のみ)。
メッシュロール:プラスアイコンをクリックして、アクセスポイントがブロードキャストするメッシュネットワークを選択します。ダイアログボックスが開きます。

   - **メッシュ:**メッシュネットワークを選択します。
   - **ロール:**選択したメッシュネットワークに対するアクセスポイントのロールを定義します。ルート アクセスポイントは、UTM に直接接続しています。初期設定を受信したメッシュ アクセスポイントは、UTM から切断されたら、メッシュネットワーク経由でルート アクセスポイントに接続します。各アクセスポイントは、1つのメッシュネットワークに対してのみメッシュ アクセスポイントとして機能できることに注意してください。

   保存すると、「*メッシュロール*」リストのアクセスポイントのアイコンがアクセスポイントのロールを示します。機能アイコンを使用してメッシュロールを編集したりリストから削除したりできます。

   重要 – 「*メッシュロール*」リストからメッシュロールを削除した場合、アクセスポイントを再度イーサネットに接続し、初期設定を取得する必要があります。アクセスポイントを再度イーサネットに接続し直さずにメッシュロールを変更するには、メッシュロールを削除しないでください。その代わり、メッシュロールの編集アイコンをクリックし、正しいメッシュネットワークを選択してください。

5. **次の詳細設定を任意で行います。**
チャネル 2.4 GHz:デフォルト設定の「*自動*」のままにすると、使用状況の一番低い送信チャネルが自動的に選択されます。固定チャネルを選択することもできます。

5 GHz チャネル（AP 50 のみで使用可能）:デフォルト設定の「*自動*」のままにすると、使用状況の一番低い送信チャネルが自動的に選択されます。固定チャネルを選択することもできます。

送信出力 2.4 GHz:アクセスポイントで最大出力で送信するためには、デフォルト設定の「*100 %*」のままにします。干渉を低減するためなど、作動距離を短縮するためには出力を低減することができます。

送信出力 5 GHz（AP 50 のみで使用可能）:AP 50 では、5 GHz 帯の送信出力を個別に低減することができます。

STP: Spanning Tree Protocol（スパニングツリープロトコル）を有効化するには、ドロップダウンリストから「*有効*」を選択します。このネットワークプロトコルは、ブリッジのループを検出して回避します。アクセスポイントがメッシュネットワークにブロードキャストする場合は STP は必ず有効にする必要があります。

VLAN タギング:VLAN を有効化するには、ドロップダウンリストから「*有効*」を選択します。VLAN タギングはデフォルトでは無効になっています。AP を既存の VLAN イーサネットインタフェースに接続するには、VLAN タギングを有効にする必要があります。VLAN イーサネットインタフェースが、「*グローバル設定 > グローバル設定*」ページの「*許可ネットワーク*」ボックスに追加されていることを確認します。

注 – ネットワーク内のアクセスポイントに対して VLAN の使用を導入するには、以下の手順に従います。標準 LAN を使用して、AP を UTM に 1分以上接続します。これは、AP が設定を取得するために必要です。最初から VLAN 経由で接続すると、AP は VLAN 内にあることを認識しないため、設定を取得するためにUTMに接続することができません。AP が表示されたら、VLAN を有効にして VLAN ID を入力します。その後、AP を目的の VLAN（スイッチなど）に接続します。

注 – AP 5 では、VLAN タギングができません。

AP VLAN ID:「*VLAN タギング*」が有効な場合、アクセスポイントがUTMに接続するために使用する VLAN の VLAN タグを入力します。VLAN タグ `0` および `1` は使用しないでください。一般に、これらのタグはネットワークハードウェア（スイッチなど）上で特別な意味を持ちます。通常、`4095` は管理用として予約されています。

注 –VLAN タギングが設定されている場合、AP は設定された VLAN に対して DHCP を 60 秒間試行します。この時間内に IP アドレスを受信できなかった場合、AP はフォールバックとして標準の LAN に DHCP を試みます。

6. **「*保存*」をクリックします。**
   アクセスポイントは、それぞれ設定または設定の更新を受信します。

   注 – 設定の変更後、すべてのインタフェースが再設定されるまで約15秒必要です。

   VLAN タギングが設定されており、AP が VLAN 経由でUTMにコンタクトできない場合、AP は自動的にリブートし、設定の受信後に再試行します。

AP へのネットワーク割り当てルール

ワイヤレスネットワークの「*クライアントトラフィック*」オプションとアクセスポイントの「*VLAN タギング*」オプションが適合する場合にのみ、アクセスポイントをワイヤレスネットワークに割り当てることができます。この際、次のルールが適用されます。

- クライアントトラフィックが「*別ゾーン*」のワイヤレスネットワーク:アクセスポイントの VLAN タギングを有効または無効にすることができます。
- クライアントトラフィックが「*AP の LAN にブリッジ*」のワイヤレスネットワーク:アクセスポイントの VLAN タギングを無効にする必要があります。
- クライアントトラフィックが「*VLAN にブリッジ*」のワイヤレスネットワーク:アクセスポイントの VLAN タギングを有効にする必要があります。それぞれのワイヤレスクライアントは、ワイヤレスネットワークに指定された「*VLAN ID にブリッジ*」を使用するか、RADIUS サーバで VLAN ID が指定されている場合は、RADIUS サーバからを受信します。

注– AP 5 は、「*クライアントトラフィック*」オプションが「*AP LAN にブリッジ*」の 1つのワイヤレスネットワークにのみ割り当てることができます。

12.3.2 グループ化

「*ワイヤレスプロテクション > アクセスポイント > グループ化*」タブで、アクセスポイントをグループ化できます。すべてのアクセスポイント グループ、またグループ化されていないアクセスポイントの概要が一覧で表示されます。アクセスポイントとグループは各アイコンによって区別されます。

アクセスポイント グループを作成するには、次の手順に従います。

1. **「グループ」ページで、「*新規グループ*」をクリックします。**
「*新規アクセスポイント グループ*」ダイアログボックスが開きます。

2. **次の設定を行います。**
名前:アクセスポイント グループを説明する名前を入力してください。

VLAN タギング:VLAN タギングはデフォルトでは無効になっています。AP を既存の VLAN イーサネットインタフェースに接続するには、チェックボックスを選択して VLAN タギングを有効にする必要があります。VLAN イーサネットインタフェースが、「*グローバル設定 > グローバル設定*」ページの「*許可ネットワーク*」ボックスに追加されていることを確認します。

- **AP VLAN ID:**この AP グループが UTM に接続するために使用する VLAN タグを入力します。VLAN タグ `0` および `1` は使用しないでください。一般に、これらのタグはネットワークハードウェア（スイッチなど）上で特別な意味を持ちます。通常、`4095` は管理用として予約されています。

アクセスポイント選択:このグループのメンバーとなるアクセスポイントを選択します。他のどのグループにも割り当てられていないアクセスポイントのみが表示されます。

ワイヤレスネットワークの選択:このグループのアクセスポイントがブロードキャストするワイヤレスネットワークを選択します。

注 – アクセスポイントがワイヤレスネットワークにブロードキャストするには、いくつか条件を満たす必要があります。詳細は、「*アクセスポイント > 概要*」の「AP へのネットワーク割り当て」セクションを参照してください。

3. **「*保存*」をクリックします。**
新しいアクセスポイントグループが「*グループ化*」リストに表示されます。

グループを編集または削除するには、対応するグループのボタンをクリックします。

アクセスポイントを編集または削除するには、対応するアクセスポイントのボタンをクリックします。アクセスポイントの編集と削除に関する詳細は、「*アクセスポイント > 概要*」を参照してください。

12.4 メッシュネットワーク

「*ワイヤレスプロテクション > メッシュネットワーク*」ページでは、メッシュネットワークを定義し、そのメッシュネットワークをブロードキャストするアクセスポイントに関連付けることができます。一般的に、メッシュネットワークでは複数のアクセスポイントが相互に通信を行い、共通のワイヤレスネットワークをブロードキャストします。1つのメッシュネットワークを介して接続された複数のアクセスポ

イントは、同じワイヤレスネットワークをクライアントにブロードキャストできるため、1つのアクセスポイントとして機能しながら広い範囲をカバーできます。また、メッシュネットワークは、ケーブルを敷設せずにイーサネットネットワーク間をブリッジするために使用することもできます。

1つのメッシュネットワークに関連付けられたアクセスポイントは、ルートアクセスポイントまたはメッシュアクセスポイントのいずれかの役割を果たします。どちらの場合もそのメッシュネットワークをブロードキャストするため、ブロードキャストできる他のワイヤレスネットワークの数は 1つ減ります。

- **ルート アクセス ポイント:**有線で UTM に接続され、メッシュネットワークを提供します。1つのアクセスポイントを複数のメッシュネットワークに対するルートアクセスポイントとすることができます。
- **メッシュ アクセス ポイント:**ルートアクセスポイントを経由して、UTM に接続するための 1つのメッシュネットワークが必要です。1つのアクセスポイントは、一度に 1つのメッシュネットワークに対するメッシュアクセスポイントとして機能します。

メッシュネットワークは、主に 2つの用途（ワイヤレスブリッジまたはワイヤレスリピーター）に使用できます。

- **ワイヤレスブリッジ:**2つのアクセスポイントを使用して、2つのイーサネットセグメント間のワイヤレス通信を確立できます。ワイヤレスブリッジは、イーサネットセグメント間をケーブルで接続できない場合に便利です。1つ目の UTM に接続されたイーサネットセグメントをルート アクセス ポイントのイーサネットインタフェースに接続し、2つ目のイーサネットセグメントをメッシュ アクセス ポイントのイーサネットインタフェースに接続する必要があります。複数のメッシュ アクセス ポイントを使用することで、さらに多くのイーサネットセグメントと接続できます。

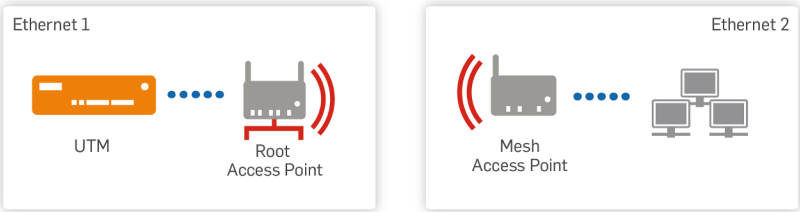

Figure 22 メッシュネットワークの使用例 – ワイヤレスブリッジ

- **ワイヤレスリピーター:**UTM に接続されたイーサネットをルート アクセス ポイントのイーサネットインタフェースに接続します。ルートアクセスポイントは、メッシュネットワークを介してメッシュ アクセス ポイントにワイヤレス接続し、メッシュアクセスポイントはワイヤレスクライアントにワイヤレスネットワークをブロードキャストします。

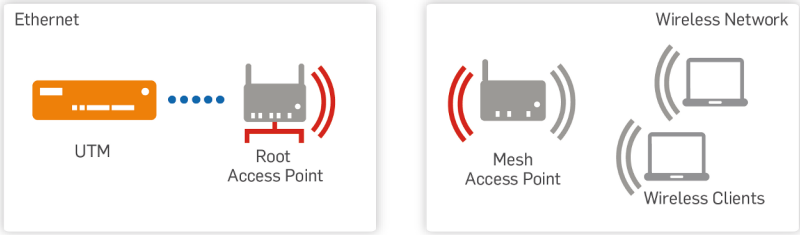

Figure 23 メッシュネットワークの使用例 – ワイヤレスリピーター

新しいメッシュネットワークを定義するには、次の手順に従います。

1. **「メッシュネットワーク」ページで「メッシュネットワークの追加」をクリックします。**
「*メッシュネットワークの追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
メッシュ ID:メッシュネットワークに対する一意の ID を入力してください。

   周波数帯:このネットワークに割り当てられたアクセスポイントは、選択した周波数帯でメッシュネットワークを伝送します。通常は、ブロードキャストされるワイヤレスネットワークとは異なる周波数帯をメッシュネットワークで使用します。

   コメント(任意):説明などの情報を追加します。

   アクセスポイント:プラスアイコンをクリックして、メッシュネットワークをブロードキャストするアクセスポイントを選択します。「*メッシュロールの追加*」ダイアログウィンドウが開きます。

   - **AP:**アクセスポイントを選択します。現在メッシュネットワークのブロードキャストに使用できるアクセスポイントは AP 50 のみです。
   - **ロール:**選択したメッシュネットワークに対するアクセスポイントのロールを定義します。ルート アクセスポイントは、UTM に直接接続しています。初期設定を受信したメッシュ アクセスポイントは、UTM から切断されたら、メッシュネットワーク経由でルート アクセスポイントに接続します。各アクセスポイントは、1つのメッシュネットワークに対してのみメッシュ アクセスポイントとして機能できることに注意してください。

注 – 初期設定で、他のアクセスポイントと同様、「*グローバル設定*」タブの「*許可インタフェース*」ボックスで選択したイーサネットセグメントのいずれかにメッシュアクセスポイントを必ず接続してください。

リストからアクセスポイントを削除するには、「*アクセスポイント*」リストの削除アイコンを使用してください。

重要 – 「*アクセスポイント*」リストからメッシュ アクセス ポイントを削除した場合、アクセスポイントを再度イーサネットに接続し、初期設定を取得する必要があります。アクセスポイントを再度イーサネットに接続し直さずにメッシュネットワークを変更するには、アクセスポイントを削除しないで、「*アクセスポイント* > *概要*」タブで、アクセスポイントの「*編集*」ボタンをクリックし、「*メッシュネットワーク*」セクションの編集アイコンをクリックし、正しいメッシュネットワークを選択してください。

アクセスポイントのアイコンがアクセスポイントのロールを示します。リストヘッダのフィルタフィールドを使用して、アクセスポイントのリスト内を検索することができます。

3. **「*保存*」をクリックします。**
   設定が保存されます。メッシュネットワークが「*メッシュネットワーク*」リストに表示されます。

12.5 ワイヤレスクライアント

「*ワイヤレスプロテクション* > *ワイヤレスクライアント*」ページは、現在アクセスポイントに接続されている(または過去に接続されていた)クライアントの概要を示します。

すべてのクライアントが名前を送信する訳ではないため、ここで名前を割り当てて、概要で既知のクライアントを識別しやすくできます。クライアントが DHCP 要求中に NetBIOS 名を送信する場合、この名前がテーブルに表示されます。送信しない場合、クライアントはリストに *[unknown]*(不明)と表示されます。これらの不明クライアントの名前は、名前の前にある鍵アイコンをクリックして変更することができます。次に、名前を入力して「*保存*」をクリックします。変更が有効になるまで数秒かかります。WebAdmin の右上隅にある「リロード」ボタンから、クライアントの名前を参照できます。

また、最初の列にある「空にする」アイコンをクリックして、クライアントをテーブルから削除することもできます。

ワイヤレスプロテクションサービスを再起動すると、「*最後の表示 (Last seen)*」タイムスタンプが消去されます。

注 – クライアントに割り当てられた IP アドレスは、UTMが該当ワイヤレスネットワークのDHCP サーバとして機能する場合にのみ表示可能です。さらに、スタティック DHCP マッピングのために、現時点では IP アドレス `0.0.0.0` が表示されます。

12.6 ホットスポット

「*ワイヤレスプロテクション > ホットスポット*」ページでは、キャプティブポータルシステムによりアクセスを管理できます。ホットスポット機能により、カフェ、ホテル、企業などではゲストに時間制限やトラフィック制限を課したインターネットアクセスを提供できます。この機能は、ワイヤレスサブスクリプション内で使用できますが、有線ネットワークでも機能します。

注 – 技術的には、ホットスポット機能により、基本的にファイアウォールで許可されているトラフィックが制限されることになります。したがって、ホットスポットを介してトラフィックを管理できるようにするためのファイアウォールルールを設定していることを確認する必要があります。ホットスポットを有効にする前に、ホットスポット機能を無効にした状態でトラフィックをテストすることをお勧めします。

ホットスポットの生成

最初に管理者は特定タイプのアクセスを備えたホットスポットを作成して有効にする必要があります。次のタイプを使用できます。

- **利用規約の許諾:**ゲストに提示する利用規約を作成できます。ゲストがホットスポットにアクセスするためには、利用規約のチェックボックスにチェックを入れる必要があります。
- **当日有効パスワード:**ゲストがホットスポットにアクセスするためには、パスワードを入力する必要があります。パスワードは毎日変更されます。
- **バウチャー:**ゲストがホットスポットにアクセスするためには、バウチャーを取得してバウチャーコードを入力する必要があります。バウチャーは、デバイスの数、時間、トラフィックで制限することができます。

ゲストへのアクセス情報の配信

「*当日有効パスワード*」および「*バウチャー*」タイプでは、アクセス情報をゲストに提供する必要があります。したがって、アクセス情報を管理して配信できるユーザを定義することができます。これらのユーザは、ユーザポータルの「*ホットスポット*」タブでアクセス情報を受信して配信します。

- **当日有効パスワード:**現在のパスワードはメールで送信したり、ユーザがユーザポータルでパスワードを確認することができます。ユーザはゲストにパスワードを転送します。ユーザは新しいパスワードを生成したり、入力することができます。新しいパスワードを設定すると、

古いパスワードが自動的に無効になり、アクティブなセッションが終了します。他のユーザには、それぞれの設定に応じて、メールまたはユーザポータルで新しいパスワードを連絡します。

- **バウチャー:**ユーザポータルでは、ユーザはそれぞれ一意のコードのバウチャーを作成できます。管理者によって指定されている場合は、異なるタイプのバウチャーを使用できます。バウチャーは印刷したりエクスポートして、ゲストに提供することができます。作成したバウチャーのリストにより、バウチャーの使用状況を把握および管理できます。

法的情報

多くの国では、公共ワイヤレス LAN の運用には、国の特定の法律が適用され、法的に疑問のあるコンテンツの Web サイト(ファイル共有サイト、過激派の Web サイトなど)へのアクセスが制限されています。この要件に準拠するためには、ホットスポットにSophos UTMの Web プロテクション機能を組み合わせて、ウェブサイトのカテゴリタイプ全体から 1つの URL までをブロックしたり、許可したりすることで、Web アクセスを制御できます。UTMを使用すると、アクセスの可能なサイトやコンテンツ、ユーザ、アクセス時間を完全に制御することができます。これにより、国や企業のポリシーによって義務付けられている場合に、ホットスポットに厳格な制限を課すことができます。

さらに、Sophos UTMの組み込み HTTP プロキシを使用しても、高度なログとレポート機能が得られます。レポートには、誰がどのサイトをいつ、何回閲覧したかが表示されるため、アクセス制限を行わずにホットスポットを運用したい場合でも、不適切な使用を特定することができます。

さらに国によっては、国の規制機関にホットスポットを登録することが義務付けられている場合があります。

12.6.1 グローバル

「*ワイヤレスプロテクション > ホットスポット > グローバル*」タブでは、ホットスポット機能を有効にし、ホットスポットアクセス情報の表示と配信を許可するユーザを定義できます。

ホットスポットを設定するには、次の手順に従います。

1. **「グローバル」タブで、ホットスポットを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、「*グローバルホットスポット設定*」エリアが編集可能になります。

2. **許可するユーザを選択します。**
   ユーザポートアルを介してホットスポットアクセス情報を提供できるユーザを選択します。ここで選択したユーザは、当日有効パスワードを変更したり、ホットスポットバウチャーを作成できます。

3. **「*適用*」をクリックします。**
   設定が保存されます。

ライブログ

ホットスポットのライブログには、ホットスポットの使用状況に関する状況が表示されます。「*ライブログを開く*」ボタンをクリックすると、新しいウィンドウでホットスポットのライブログが開きます。

12.6.2 ホットスポット

「*ワイヤレスプロテクション > ホットスポット > ホットスポット*」タブでは、各種のホットスポットを管理できます。

注 – ホットスポットは、WLAN インタフェースなどの既存のインタフェースに割り当てる必要があります。このインタフェースを使用するすべてのホストは、ホットスポットにより自動的に制限されます。したがって、通常ホットスポットを作成する前に クライアントトラフィックが「*別ゾーン*」のワイヤレスネットワークを作成してから、各 WLAN インタフェースハードウェアのインタフェースを作成します。詳しくは、「*ワイヤレスプロテクション > ワイヤレスネットワーク*」を参照してください。

ホットスポットを作成するには、次の手順に従います。

1. **「*ホットスポットの追加*」をクリックします。**
   「*ホットスポットの追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このホットスポットを説明する名前を入力してください。

   インタフェース:ホットスポットにより制限するインタフェースを追加します。選択したインタフェースに対して、必要なトラフィックを許可するファイアウォールルールが設定されていることを確認してください。インタフェースは、1つのホットスポットでのみ使用できます。

   警告 – ここではアップリンクインタフェースを選択しないでください。インターネットへのトラフィックが後に完全にブロックされてしまいます。また、認証などの重要なサービスを提供

するサーバが使用するインタフェースは使用しないことを強く推奨します。WebAdmin からロックアウトされ、解除できなくなる恐れがあります。

ホットスポットタイプ:選択したインタフェースのホットスポットタイプを選択します。

- **当日有効パスワード:**新しいパスワードが 1日に 1回自動的に作成されます。このパスワードは、ユーザポータルの「*ホットスポット*」タブに表示されます。これは、「*グローバル*」タブに指定されているすべてのユーザに提供されます。さらに、指定したメールアドレスにも送信されます。
- **バウチャー:**(ベーシックガード サブスクリプションでは、利用できません。)このホットスポットタイプでは、さまざまな制限とプロパティを持つユーザポータルのトークンを作成、印刷してユーザに提供することができます。ユーザがコードを入力すると、インターネットに直接アクセスできます。
- **利用規約の許諾:**ユーザは利用規約を許諾した後にインターネットにアクセスできます。

パスワード作成時刻(「*当日有効パスワード*」のホットスポットタイプのみ):新しいパスワードが作成される時刻を指定。この時刻になると、古いパスワードが即時に無効になり、現在のセッションが切断されます。

パスワードのメール送信先(「*当日有効パスワード*」のホットスポットタイプのみ):パスワードの送信先のメールアドレスを追加します。

バウチャー定義(「バウチャー」のホットスポットタイプのみ):このリストには、指定されているバウチャー定義が表示されます。ホットスポットに使用する定義を選択します。

バウチャー当たりのデバイス(「バウチャー」のホットスポットタイプのみ):バウチャーの有効期間中に 1つのバウチャーでログインを許可するデバイス数を入力します。これを*無制限(unlimited)*にすることは推奨されません。

セッション期限(「*当日有効パスワード*」のホットスポットタイプのみ):アクセスの有効期限を入力します。この時間が過ぎると、ユーザは利用規約を再度受諾してログインする必要があります。

ユーザに利用規約の許諾を求める(「*当日有効パスワード*」または「バウチャー」のホットスポットタイプのみ):ホットスポットユーザがインターネットにアクセスする前に、ユーザに利用規約を許諾してもらう場合は、このオプションを選択します。

- **利用規約:**利用規約として表示するテキストを追加します。シンプルな HTML マークアップとハイパーリンクを使用できます。

ログイン後 URL に転送:選択すると、パスワードまたはバウチャーデータの入力後、ユーザは、ホテルの Web サイトまたはポータルのシステムポリシーが記載された Web ページなど、指定の URL に自動的に転送されます。

- **URL:**ユーザが転送される転送先 URL。

コメント(任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   ロゴを削除:ログインページからロゴを削除します。

   新規ロゴのアップロード:ログインページにタイトルを追加します。

   タイトル:ログインページにタイトルを追加します。シンプルな HTML マークアップとハイパーリンクを使用できます。

   カスタムテキスト:ログインページにテキストを追加します。使用するワイヤレスネットワークの SSID などを入力できます。シンプルな HTML マークアップとハイパーリンクを使用できます。

   注 –「*タイトル*」および「*カスタムテキスト*」は、「*詳細*」タブでそれぞれのチェックボックスがチェックされている場合にバウチャーに印刷されます。

4. **「*保存*」をクリックします。**
   ホットスポットが作成され、ホットスポットリストに表示されます。

ヒント – ホットスポットを保存した後、ログインページのプレビューを開くことができます。ホットスポットリストで各ホットスポットの「*ログインページをプレビュー*」ボタンをクリックします。

ホットスポットを編集または削除するには、対応するボタンをクリックします。

12.6.3 バウチャー定義

「*ワイヤレスプロテクション > ホットスポット > バウチャー定義*」タブでは、バウチャータイプのホットスポットの各種バウチャー定義を管理できます。

バウチャー定義を作成するには、次の手順に従います。

1. **「*バウチャー定義の追加*」をクリックします。**
   「*バウチャー定義の追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このバウチャー定義を説明する名前を入力します。

有効期限:この定義のバウチャーの有効期間を指定します。このカウントは初回ログイン時から始まります。必ずこの期限を設定することをお勧めします。

時間割当:ここでは、許可するオンライン時間を制限できます。この定義のバウチャーの期限が切れるまでの最大オンライン時間を指定します。このカウントはログイン時から始まり、ログアウト時に停止します。さらに、5分間にわたってアクティビティがない場合にカウントが停止します。

データボリューム:ここでは、許可するデータボリュームを制限できます。このバウチャー定義で送信できる最大データ量を入力します。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   バウチャー定義が作成されます。バウチャータイプのホットスポットの作成時には、このバウチャー定義を選択できるようになります。

バウチャー定義を編集または削除するには、対応するボタンをクリックします。

12.6.4 詳細

バウチャー印刷オプション

ページサイズ:ユーザポータルで印刷するバウチャーのサイズを選択します。

ページ当たりのバウチャー数:1ページに印刷するバウチャーの数を指定します。

印刷タイトル/カスタムテキストの印刷:バウチャーにタイトルまたはカスタムテキストを印刷する場合に選択します。タイトルおよびテキストは、「*ログインページカスタマイズ*」セクションの「*ホットスポット*」タブで各ホットスポットに対して定義します。

バウチャー一般オプション

ここには、期限切れになったバウチャーをデータベースから削除するかどうか、削除する場合は何日後に削除するかを指定できます。ホットスポットのログには、引き続き削除されたバウチャーの情報が表示されます。

Walled Garden

パスワードやバウチャーコードを入力しなくても、すべてのユーザが常にアクセスできる特定のホストまたはネットワークを追加します。

13 Web サーバプロテクション

この章では、Web サーバを攻撃や悪意ある行為から保護するSophos UTMの Web アプリケーションファイアウォールを設定する方法を説明します。

この章では、次のトピックについて説明します。

- WAF
- 証明書管理

13.1 WAF

Sophos UTMで Web アプリケーションファイアウォール（WAF、あるいはリバースプロキシ）を使用すると、Web サーバをクロスサイトスクリプティング（XSS）、SQL インジェクション、ディレクトリトラバーサルなどの攻撃や悪意ある行為、あるいはその他の潜在的な攻撃から防御することができます。DNAT ルールを使用して本当のマシンに変換される外部アドレス（仮想サーバ）を定義することができます。ここで、様々なパターンと検出方法を使用して、サーバを保護することができます。簡単に言うと、UTMのこのエリアでは、Web サーバから送受信されるリクエストに、利用条件を適用することができます。また、複数のターゲットの間でのロードバランシングが可能になります。

13.1.1 グローバル

「*WAF > グローバル*」タブでは、Web アプリケーションファイアウォール（WAF）を有効または無効にできます。

注 – WAF を有効にする前に、「*仮想 Web サーバ*」タブで仮想 Web サーバを 1つ以上作成する必要があります。

WAF を有効にするには、次の手順に従います。

1. **バックエンドWebサーバまたは仮想 Web サーバを 1つ以上作成します。**
   詳しくは、「バックエンドWebサーバ」と「仮想 Web サーバ」のセクションを参照してください。
2. **Web アプリケーションファイアウォールを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、Web アプリケーションファイアウォールが有効になります。

ライブログ

WAF ライブログは、WAF イベントに関するデバッグ情報を提供します。「*ライブログを開く*」ボタンをクリックすると、新しいウィンドウで WAF ライブログが開きます。

13.1.2 仮想 Web サーバ

「*WAF > 仮想 Web サーバ*」タブでは、仮想 Web サーバを作成できます。これらの Web サーバは、UTMの一部として、インターネットとWeb サーバの間のファイアウォールを構築します。そのため、このような介入をリバースプロキシとも呼びます。UTMは、Web サーバへのリクエストをピックアップし、バックエンドWebサーバを様々な攻撃から保護します。それぞれの仮想サーバはバックエンドWebサーバにマッピングされており、どのような保護レベルを適用するかを決定します。また、複数のバックエンドWebサーバを 1つの仮想 Web サーバ定義で使用することもできます。これにより、バックエンドWebサーバのロードバランシングを実行できます。

仮想サーバを追加するには、次の手順に従います。

1. **「*新規仮想 Web サーバ*」ボタンをクリックします。**
   「*新規仮想 Web サーバを作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:仮想 Web サーバを説明する名前を入力してください。

   インタフェース: Web サーバに到達するために使用するインタフェースをドロップダウンリストから選択します。

   タイプ:クライアントと仮想 Web サーバの間の通信を暗号化するか (HTTPS) しないか (HTTP) を決定します。

   ポート:仮想 Web サーバに外部から到達可能なポート番号を入力します。デフォルトはポート80 (*HTTP*) とポート443 (*HTTPS*) です。

   証明書 (*HTTPSのみ*):ドロップダウンリストから Web サーバの証明書を選択します。証明書は事前に Web サーバ上に作成し、「*証明書管理 > 証明書*」タブでアップロードしておく必要があります。

      ドメイン:このフィールドには、証明書の作成されるホスト名が表示されます。

      ドメイン (SAN 証明書のみ):WAFは、SAN (Subject Alternative Name) 証明書をサポートします。証明書でカバーされるすべてのホスト名がこのボックスにリストされます。続いて、ホスト名の前にあるチェックボックスにチェックを入れて、複数のホスト名を選択することができます。

ドメイン(*HTTP のみ*):Web サーバが責任を持つドメインを FQDN として入力します(例: `shop.example.com`)。

バックエンドWebサーバ:ファイアウォールプロファイルを適用する Web サーバの前にあるチェックボックスにチェックを入れます。ミラーリング Web サーバがある場合、複数の Web サーバを選択することもできます。デフォルトでは、選択した Web サーバ間でトラフィックのロードバランシングが行われます。リクエストのカウントアルゴリズムにより、各新規リクエストが、現在有効なリクエスト数が一番少ない Web サーバに自動で割り当てられます。「*サイトパスルーティング*」タブでは、詳細な負荷分散ルールを指定できます。

ファイアウォールプロファイル:ドロップダウンリストからファイアウォールプロファイルを選択します。このプロファイルは、選択した Web サーバを保護するために適用されます。また、ファイアウォールプロファイルを一切使用しない場合は「*プロファイルなし*」を選択できます。

HTML リライティングを有効化 (オプション):このオプションを選択すると、返された Web ページのリンクをが書き換えるため、リンクが有効に保たれます。例:バックエンドWebサーバのインスタンスの 1つが、`yourcompany.local`というホスト名であるが、UTMでの仮想サーバのホスト名が`yourcompany.com`である。したがって、`<a href="http://yourcompany.local/">` のような絶対リンクは、クライアントへの配信前にリンクを `<a href="http://yourcompany.com/">` に書き換えなければ破損してしまいます。ただし、Web サーバで `yourcompany.com` が設定されているか、Web ページの内部リンクが常に相対リンクとして表現されている場合には、このオプションを有効にする必要はありません。Microsoft の Outlook Web Access や Sharepoint Portal Server では、このオプションを使用することを推奨します。

注 – 一部のリンクが正しく書き換えられず、無効となる場合もあります。リンクを一貫してフォーマットするよう、Web サイトの作者に依頼してください。

URL リライティングとは別に、HTML リライティング機能でも、正しくフォーマットされていない HTML を次のように修正することができます。

- DOM ツリーで、`<title>` タグを、ノード `html > title` から正しい `html > head > title` に移動する
- HTML 属性値を囲む引用符を修正する(例: `name="value""` が `name="value"` になる)

注 – HTML リライティングは、HTTP コンテンツタイプが `text/*` または `*xml*`(*はワイルドカード)のすべてのファイルに影響します。バイナリファイルなどの他のファイルタイプの HTTP コンテンツタイプが正しいことを確認してください。コンテンツタイプが間違っていると、HTML リライティング機能により破損する可能性があります。

クロスリファレンス – 詳しくは、libxmlド キュメントを参照してください (http://xmlsoft.org/html/libxml-HTMLparser.html)。

ホストヘッダをパス(オプション):このオプションを選択すると、クライアントに要求されたホストヘッダが保持され、Web リクエストとともに Web サーバへ転送されます。環境内で、ホストヘッダの受け渡しが必要かどうかは、Web サーバの設定に応じて決まります。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   サーバが「*仮想 Web サーバ*」リストに追加されます。

仮想サーバに複数の Web サーバが設定されている場合、「*仮想 Web サーバ*」リストには、各 Web サーバのステータスアイコンが表示されます。Web サーバのステータスアイコンは、サーバが有効でない場合は赤くなります。Web サーバがダウンしているか利用できない場合は赤色、すべて正常に機能している場合は緑色です。

13.1.3 バックエンドWebサーバ

「*WAF > バックエンドWebサーバ*」タブで、WAF によって保護する Web サーバを追加できます。

Web サーバを追加するには、次の手順に従います。

1. **「*新規バックエンドWebサーバ*」ボタンをクリックします。**
   「*新規バックエンドWebサーバを作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:Web サーバを説明する名前を入力してください。

   ホスト:ホストを追加または選択します。ホストは、タイプが「*ホスト*」または「*DNS ホスト*」です。ここでは、DNS ホスト名の使用を強く推奨します。これは、IP アドレスでリストされたホストは空のホストヘッダを送信するため、一部のブラウザで問題が発生するためです。

   タイプ:UTM とWeb サーバの間の通信を暗号化するか (HTTPS) しないか (HTTP) を決定します。

ポート:UTM とWeb サーバの間の通信に使用するポート番号を入力します。デフォルトはポート80(*HTTP*)とポート443(*HTTPS*)です。

コメント(任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   HTTP キープアライブの使用:デフォルトでは、WAF は HTTP キープアライブを使用します。つまり、HTTP の持続的接続をすることで、CPU やメモリの使用率の削減につながります。まれにバックエンドWebサーバで HTTP キープアライブがが正しく機能しないことがあり、読み込みエラーやタイムアウトが起こることがあります。その場合は、該当の Web サーバでこの機能を無効にする必要があります。仮想 Web サーバに対して、HTTP キープアライブ機能が無効になっているバックエンドWebサーバが少なくとも 1台割り当てられている場合、この仮想 Web サーバに割り当てられているすべてのバックエンドWebサーバでこの機能は自動的に無効になります。
4. **「*保存*」をクリックします。**
   サーバが「*バックエンドWebサーバ*」リストに追加されます。

これで「*仮想 Web サーバ*」タブで存在する Web サーバをファイアウォールプロファイルに割り当てられるようになります。

13.1.4 ファイアウォールプロファイル

「*WAF > ファイアウォールプロファイル*」タブでは、Web サーバの保護モードとレベルを定義する WAF プロファイルを作成できます。

WAF プロファイルを作成するには、以下の手順に従います。

1. **「*新規ファイアウォールプロファイル*」ボタンをクリックします。**
   「*ファイアウォールプロファイルの作成*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前:プロファイルを説明する名前を入力してください。

   Outlook Anywhere をパス:外部の Microsoft Outlook クライアントに対し、WAF 経由で Microsoft Exchange Server へのアクセスを許可します。Microsoft Outlook のトラフィックは WAF によるチェックや保護を受けません。

   モード:ドロップダウンリストからモードを選択します。

   - **モニタ:**HTTP リクエストをモニタリングし、ログに記録します。
   - **リジェクト:**HTTP リクエストは拒否されます。

- **破棄:**HTTP リクエストは破棄されます。

選択したモードは、HTTP リクエストが下で選択したいずれかの条件と合致している場合に適用されます。

クロスサイトスクリプティング (XSS) フィルタ: Web サーバをクロスサイトスクリプティングから保護します。このために、HTML フォームやその他の入力フィールドが、パーサによって、HTML および CSS コマンドを使用してチェックされます。

SQL インジェクションフィルタ: Web サーバを SQL インジェクションから保護します。このために、HTML フォームやその他の入力フィールドが、パーサによって、SQL コマンドを使用してチェックされます。

Cookie 署名: Web サーバを Cookie の悪用から保護します。Web サーバが Cookie をセットすると、最初の Cookie に対して 2つ目の Cookie が追加されます。この Cookie には、最初の Cookie の名前、値、シークレットから構成されたハッシュが含まれており、シークレットは WAF によってのみ認識されます。したがって、リクエストによって正しい Cookie ペアが提供されない場合は、ある種の悪用が行われた可能性があり、Cookie は破棄されます。

URL ハードニング:URL 書き換えから保護します。このために、クライアントが Web サイトを要求すると、この Web サイトのすべての URL に対して署名が行われます。この署名手順は、Cookie 署名と似ています。さらに、次にどのリンクを有効に要求できるのかについて、Web サーバからの応答が解析されます。ハードニングされた URL をブックマークし、後でアクセスすることができます。エントリ URL を定義する方法を、以下のいずれかから選択します。

- **エントリ URL を手動で指定:**Web サイトのエントリ URL として機能する URL を入力します。これにより、署名が不要になります。これらの URL は、`http://shop.example.com/products/`、`https://shop.example.com/products/`、または `/products/` という構文に準拠している必要があります。
- **アップロードした Google サイトマップファイルからのエントリ URL:**ここで、Web サイトの構造に関する情報が含まれるサイトマップファイルをアップロードします。サイトマップファイルは、XML 形式でもプレーンテキスト形式でもアップロードできます。後者のファイルは URL のリストのみが含まれます。プロファイルを保存すると、サイトマップファイルは WAF によって構文解析されます。
- **Google サイトマップ URL からのエントリ URL:**UTM に、Web サイトの構造に関する情報が含まれるサイトマップファイルを、定義された URL からダウンロードさせることができます。このファイルにアップデートがないか定期的にチェックすることができます。プ

ロファイルを保存すると、サイトマップファイルはダウンロードされ、WAF によって構文解析されます。
URL:サイトマップへのパスを絶対 URL として入力します。

更新:ドロップダウンリストから更新間隔を選択します。「*手動*」を選択すると、サイトマップはこのプロファイルの更新を保存した場合にのみ更新されます。

注 – URL ハードニングは、HTTP コンテンツタイプが `text/*` または `*xml*`(*はワイルドカード)のすべてのファイルに影響します。バイナリファイルなどの他のファイルタイプの HTTP コンテンツタイプが正しいことを確認してください。コンテンツタイプが間違っていると、URL ハードニング機能により破損する可能性があります。

フォームハードニング: Web フォームの書き換えから保護します。フォームハードニングは、Web フォームのオリジナル構造を保持し、署名します。そのため、フォームの送信時にフォームの構造が変更されると、サーバは要求を拒否します。

注 – フォームハードニングは、HTTP コンテンツタイプが `text/*` または `*xml*`(*はワイルドカード)のすべてのファイルに影響します。バイナリファイルなどの他のファイルタイプの HTTP コンテンツタイプが正しいことを確認してください。コンテンツタイプが間違っていると、フォームハードニング機能により破損する可能性があります。

アンチウイルススキャン:このオプションを選択して、Web サーバをウイルスから防御します。

AV エンジン: Sophos UTMSophos UTM は、最高のセキュリティを実現するさまざまなアンチウイルスエンジンを備えています。

- **シングルスキャン:**デフォルト設定。「スキャン設定」タブに定義されたエンジンを使用して最高レベルのパフォーマンスを実現します。
- **デュアルスキャン:**各トラフィックに対し、異なるウイルススキャナを使用してスキャンを 2回行うことにより、検出率を最大限に高めます。ベーシックガードサブスクリプションではデュアルスキャンは利用できません。

スキャン:ドロップダウンリストから、アップロードまたはダウンロードのいずれかをスキャンするか、その両方をスキャンするかを選択します。

スキャン不可コンテンツのブロック:このオプションを選択して、スキャンできないファイルをブロックします。スキャンできない理由はいくつかありますが、ファイルが暗号化されているか、破損している可能性があります。

低レピュテーションのクライアントをブロック: GeoIP および RBL 情報に基づいて、評判の悪いクライアントを分類に従ってブロックすることができます。Sophosでは次の分類プロバイダを利用します。

RBL ソース:

- Commtouch IP Reputation(ctipd.org)
- dnsbl.proxybl.org
- http.dnsbl.sorbs.net

GeoIP ソースは Maxmind です。WAF は、次のいずれかの Maxmind カテゴリに属するクライアントをブロックします。

- A1:クライアントによって、IP アドレスや本来の所在地を隠すために使用される匿名プロキシまたは VPN サービス。
- A2:衛星プロバイダとは、衛星を利用して世界中の(多くの場合、高リスクな国の)ユーザにインターネットアクセスを提供しているISP です。

コメント(任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
WAF ルールのスキップ:このボックスに、誤検出などが理由で現在のプロファイルでスキップしたい WAF ルール番号を追加します。これらの WAF ルール番号は、「*ログとレポート > WAF > 詳細*」ページで、「*上位ルール*」フィルタを使用して取得できます。

低レピュテーションのクライアントに対するリモートルックアップをスキップ:評判ルックアップにはリモート分類プロバイダへの要求の送信が含まれるため、評判に基づくブロック機能を使用すると、システムのパフォーマンスが低下する可能性があります。このチェックボックスは、GeoIP に基づく分類を使用する場合にのみ、チェックを入れてください。この場合、キャッシュされた情報を使用するため、パフォーマンスは大幅に向上します。

4. **「*保存*」をクリックします。**
新しい WAF プロファイルが「*ファイアウォールプロファイル*」リストに追加されます。

URL ハードニングとフォームハードニングに関する追加情報

URL ハードニングとフォームハードニングの両方を有効化することを推奨します。これら 2つの機能は相補的なので、いずれか一方だけ有効化した場合に起こり得る問題を解決することができます。

- フォームハードニングだけ有効化した場合:`http://example.com/?view=article&id=1` などのように、Web ページに追加クエ

リの付いたハイパーリンクが含まれている場合（特定の CMS など）、このようなページ要求は、フォームハードニングが署名を探してしまい、その署名が見つからないためにブロックされます。

- URLハードニングだけ有効化した場合:Web ブラウザがフォームデータを Web フォームの `form` タグのアクション URL に追加する場合（GET 要求など）、フォームデータは Web サーバに送信される要求 URL の一部となり、URL 署名が無効になります。

両方の機能を有効化することで問題が解決するのは、フォームハードニングと URL ハードニングのいずれかが要求を有効だとみなすと、サーバが要求を受け付けるためです。

Outlook Web Access

Outlook Web Access（OWA）用の WAF の構成はややリスクを伴います。これは、OWA がパブリック IP からの要求を、内部 LAN IP からの OWA Web サイトへの要求とは別の方法で処理するためです。OWA の URL にはリダイレクトが追加されます。外部アクセスのためには外部 FQDN が使用されますが、内部要求には内部サーバの IP アドレスが使用されます。

解決策は、OWA Web サーバの WAF プロファイルで、OWA ディレクトリを*エントリ URL* として設定することです（例: `http://webserver/exchange/`）。さらに、パス `/exchange/*` の URL ハードニングをスキップする除外を作成し、Cookie 署名を仮想サーバに対して完全に無効化する必要があります。

13.1.5 除外

「*WAF > 除外*」タブでは、特定のチェックから除外される Web リクエストや送信元ネットワークを定義できます。

1. **「*除外*」タブで、「*新規除外リスト*」をクリックします。**
   「*除外リストを作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:除外を説明する名前を入力してください。

   コメント（任意）:説明などの情報を追加します。

   実行しないチェック:スキップするセキュリティチェックを選択します。

   対象仮想 Web サーバ:ドロップダウンリストから、選択されたチェックから除外する仮想 Web サーバを選択します。

   対象リクエスト:ドロップダウンリストから要求の定義を選択します。AND または OR を使用して、2つの要求の定義を論理的に組み合わせることができます。

ネットワーク:クライアント要求の発信元であり、選択されたチェックから除外する送信元ネットワークを追加または選択します。

パス:選択されたチェックから除外するパスを、`/products/images/*` のような形式で追加します。

3. **次の詳細設定を任意で行います。**
   URL/フォームハードニング実行時に HTML を変更しない:選択すると、定義した除外設定と一致するデータがWAFエンジンにより変更されません。このオプションを使用すると、本 Web サーバにより正しくないテキスト/HTML コンテンツが提供されたバイナリデータが破損することがありません。その一方で、有効化された URL ハードニング、HTML リライティング、またはフォームハードニングによって Web リクエストがブロックされることがあります。これらの 3 つの機能は HTML パーサーを使用するため、ある程度 Web ページコンテンツの変更に依存します。望ましくないブロックを回避するには、ブロックの影響を受ける要求に対して URL ハードニング/フォームハードニングをスキップします。この設定は、Web サーバや Web ページの依存関係に応じて、別の除外か新しい除外で行うことが必要な場合があります。

4. **「*保存*」をクリックします。**
   新しい除外が「*除外*」リストに表示されます。

5. **除外リストを有効にします。**
   新しい除外はデフォルトで無効になっています(トグルスイッチはグレー表示)。例外を有効にするには、トグルスイッチをクリックします。

   これで除外リストが有効になります(トグルスイッチは緑色)。

除外ルールを編集または削除するには、対応するボタンをクリックします。

13.1.6 サイトパスルーティング

「*WAF > サイトパスルーティング*」タブでは、外部から受信したリクエストを転送するバックエンドWeb サーバを定義できます。たとえば、`/products` などの特定パスのすべての URL を特定 Web サーバに送信することを定義できます。また、特定のリクエストに複数の Web サーバを許可する一方で、これらのサーバ間でリクエストを分散するためのルールを追加することもできます。たとえば、セッションの有効期間を通して各セッションを 1つの Web サーバに関連付けること(スティッキーセッション)を定義できます。これは、オンラインショップをホストしている場合に、ユーザがショッピングセッション中に使用するサーバを 1台に固定するためなどに必要になります。さらに、すべてのリクエストを 1台の Web サーバに送信して、他のサーバをバックアップとしてのみ使用するように設定することもできます。

各仮想 Web サーバには、1つのデフォルトサイトパスルート(/ のパス)が自動的に作成されます。UTMでは、最も妥当な方法でサイトパスルートを自動的に適用し、最も厳格なパス、つまり最長のパスから始めて、他の特定サイトパスルートが外部から受信したリクエストと一致しない場合にのみ使用されるデフォルトパスルートまで順に適用します。サイトパスルートリストの順序は重要ではありません。デフォルトルートが削除された場合など、受信したリクエストに一致するルートがない場合は、リクエストが拒否されます。

注 –「*サイトパスルーティング*」タブは、1つ以上のリアバックエンドWebサーバと1つ以上の仮想サーバが作成されている場合にのみアクセスできます。

サイトパスルートを作成するには、次の手順に従います。

1. **「*新規サイトパスルート*」ボタンをクリックします。**
   「*新規サイトパスルートを作成*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   対象仮想 Web サーバ:受信トラフィックの元のターゲットホストを選択します。

   このパス用に全リクエストを送信:`/products`など、サイトパスルートを作成するパスを入力します。

   バックエンドWebサーバ:指定するパスに使用するバックエンドWebサーバの前にあるチェックボックスにチェックを入れます。選択されているサーバの順序は、「*ホットスタンバイモードでバックエンドを処理*」オプションでのみ意味があります。ソートアイコンを使用すると、順序を変更できます。

   コメント(任意):説明などの情報を追加します。

3. **次の詳細設定を任意で行います。**
   スティッキーセッション cookie によりバックエンドを選択:各セッションを 1つのバックエンドWebサーバに関連付ける場合に、このオプションを選択します。これを有効にすると cookie がユーザのブラウザに渡され、これによりこのブラウザからのすべての要求を同じバックエンドWebサーバにルーティングするようUTMに指示が出されます。サーバが使用できない場合には、cookie が更新されず、セッションが別の Web サーバに切り替わります。

   ホットスタンバイモードでバックエンドを処理:すべてのリクエストを最初に選択したバックエンドWebサーバに送信し、他の Web サーバをバックアップとしてのみ使用する場合は、このオプションを選択します。バックアップサーバは、メインサーバに障害が発生した場合にのみ使用されます。「*スティッキーセッション cookie によりバックエンドを選択*」オプションを選択していない限り、メインサーバが復旧するとすぐにセッションがメインサーバに戻ります。

4. **「*保存*」をクリックします。**
   サイトパスルートが「*サイトパスルート*」リストに追加されます。

サイトパスルートを編集または削除するには、対応するボタンをクリックします。

13.1.7 詳細

「*WAF > 詳細*」タブでは、cookie の署名と URL ハードニングに使用するキーを定義できます。

Cookie 署名キー

ここでは、Cookie 署名用の署名キーとして使用できるカスタムのシークレットを入力できます。

URL ハードニング署名キー

ここでは、URL ハードニング用の署名キーとして使用されるカスタムのシークレットを入力できます。

フォームハードニング設定

ここでは、フォームハードニングトークンの暗号キーとして使用されるカスタムのシークレットを入力できます。シークレットは 8文字以上にする必要があります。

13.2 証明書管理

「*サイト間 VPN > 証明書管理*」メニューと「*Web サーバプロテクション > 証明書管理*」メニューには、同じ設定オプションが含まれています。これらの設定オプションを使用すると、Sophos UTMのすべての証明書関連オプションを管理することができます。たとえば、X.509 証明書の作成またはインポートや、CRL *(証明書失効リスト)*のアップロードなどを行うことができます。

13.2.1 証明書

「*サイト間 VPN > 証明書管理 > 証明書*」を参照してください。

13.2.2 認証局 (CA)

「*サイト間 VPN > 証明書管理 > CA*」を参照してください。

13.2.3 証明書失効リスト(CRL)

「*サイト間 VPN > 証明書管理 > 証明書失効リスト(CRL)*」を参照してください。

13.2.4 詳細

「*サイト間 VPN > 証明書管理 > 詳細*」を参照してください。

14 RED マネジメント

この章では、Sophos RED の設定方法について説明します。RED は*リモートイーサネットデバイス (Remote Ethernet Device)*の略で、リモートオフィス(遠隔地の支店)などを、あたかもローカルネットワークの一部であるかのようにメインオフィス(本社)に接続する手段です。

セットアップは、メインオフィスのSophos UTMとリモートオフィスのリモートイーサネットデバイス(RED)で構成されます。RED アプライアンス自体は設定する必要がないため、2拠点間の接続は非常に簡単に確立できます。RED アプライアンスは、UTMに接続するとただちに、UTM上の他のイーサネットデバイスと同じように動作します。ブランチオフィスのすべてのトラフィックはを介して安全にUTMルーティングされるため、支社・支店はローカルネットワークと同じように安全になります。

現在 2種類の RED アプライアンスを利用できます。

- RED 10:小規模オフィス向け RED ソリューション
- RED 50:支店を含む規模の大きいオフィス向け RED ソリューション(2つのアップリンクインタフェースを設置)

この章では、次のトピックについて説明します。

- 概要
- グローバル設定
- クライアントマネジメント
- 導入ヘルパ
- トンネルマネジメント

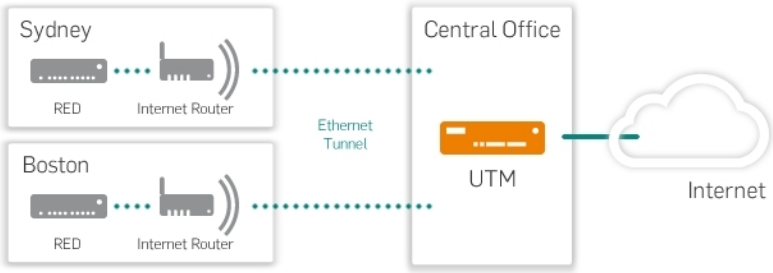

Figure 24 RED:セットアップの略図

RED 環境のセットアップは、以下の手順で行います。

1. RED サポートをアクティブにします。
2. UTM上で RED アプライアンスを設定します。
3. RED アプライアンスをリモートサイト上のインターネットに接続します。

注 – RED アプライアンスが設定されていないと、RED の概要ページには、RED アーキテクチャの一般的な情報が表示されます。RED アプライアンスを設定すると、そのページには RED のステータスに関する情報が表示されます。

14.1 概要

「*概要*」ページは、RED の概要、その機能、および一般的な RED のセットアップについて基本情報を示します。

参照 – RED デバイスの詳細については、「Sophos UTMリソースセンター」の「*クイックスタートガイド*」および「*取扱説明書*」を参照してください。RED 10 アプライアンスの LED ブリンクコードは、Sophosサポートデータベースを参照してください。

RED ライブログを開く

ライブログを使用して、Sophos UTMと RED アプライアンスの間の接続をモニタリングすることができます。「*RED ライブログを開く*」ボタンをクリックすると、新しいウィンドウでライブログを開きます。

14.2 グローバル設定

「*グローバル設定*」タブでは、RED のサポートを有効または無効にすることができます。RED のサポートを有効にすると、UTMがRED ハブとして機能します。RED サポートは、RED アプライアンスをUTMに接続する前に有効にしておく必要があります。

RED 設定

RED サポートを有効にするには、次の手順に従います。

1. **「*グローバル設定*」タブで、RED サポートを有効化します。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*RED ハブ設定*」エリアが編集可能になります。

2. **組織の詳細を入力します。**
   デフォルトで、「*マネジメント > システム設定 > 組織*」タブの設定が使用されます。

3. **「*RED の有効化*」をクリックします。**
   トグルスイッチが緑色になり、RED サポートが有効になります。これで UTM が Sophos の RED プロビジョニングサービス (RPS) に登録され、RED ハブとして機能するようになります。

   「*クライアントマネジメント*」ページで 1つ以上の RED アプライアンスを追加して続行するか、*導入ヘルパ*のウィザードを使用することができます。

設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

デバイスの自動認証解除

RED サポートが有効になっている場合、一定時間経過後、切断された RED アプライアンスが自動的に認証解除されるように設定することができます。この機能により、盗難に遭った RED アプライアンスが UTM に接続できないようにします。

1. **自動認証解除を有効にします。**
   「*デバイスの自動認証解除*」チェックボックスを選択します。

2. **RED アプライアンスが認証解除されまでの時間を指定します。**
   指定の時間を「*認証解除するまでの時間*」テキストボックスに入力します。最小設定時間は 5分です。

3. **「*適用*」をクリックします。**
   これでデバイスの自動認証解除が有効になります。

RED アプライアンスが指定した時間を超えて接続が切断された後再接続すると、自動的に無効化されます。これは「*クライアントマネジメント*」ページのトグルスイッチでも示されます。また、「*概要*」ページにも該当する警告が表示されます。認証解除された RED アプライアンスに再度接続を許可するには、「*クライアントマネジメント*」ページで RED アプライアンスを有効化します。

14.3 [サーバ] クライアントマネジメント

「*RED マネジメント > クライアントマネジメント*」ページでは、RED トンネルを使用して UTM に接続するために、リモート UTM を有効化することができます。これにより UTM は RED アプライアンスのように機能するようになります。さらにここでは、導入ヘルパを使用する代わりに、RED アプライアンスを手動で設定することができます (エキスパートモード)。導入ヘルパは、RED アプライアンスの設定に使用できるより便利な機能で、次の WebAdmin ページに提供されています。

ここで設定した各 RED アプライアンスまたは各UTMは、UTMとの接続を確立できるようになります。

ページ名の前に*[サーバ]*タグが付いている場合は、UTMをサーバ (RED ハブ) として機能させる場合にのみ、このページの設定が必要になることを表しています。

注 – RED アプライアンスの接続を可能にするためには、まず「*グローバル設定*」ページで RED サポートを有効にする必要があります。

2台のUTM間での RED トンネルのセットアップ

RED トンネルを使用してローカルUTMに接続するために別のUTMを有効にするには、次の手順に従います。

1. **「*クライアントマネジメント*」タブで、「*RED の追加*」をクリックします。**
   「*RED の追加*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   ブランチ名:クライアント UTM が配置されたブランチ名を入力します (例:「ミュンヘンオフィス」)。

   クライアントタイプ:ドロップダウンリストから「*UTM*」を選択します。

   トンネル ID:デフォルトでは「*自動*」が選択されています。トンネルには順番に番号が付けられます。両方のUTMのトンネル ID が一意であることを確認する必要があります。重複する場合は、ドロップダウンリストから別の ID を選択す必要があります。
3. **「*保存*」をクリックします。**

   UTMオブジェクトが生成されます。
4. **プロビジョニングファイルをダウンロードします。**
   リモート (クライアント)UTM に設定データを送るには、「*ダウンロード*」ボタンを使用してプロビジョニングファイルをダウンロードし、安全な手段でリモートUTMにファイルを送信します。

RED アプライアンスの設定

ローカルUTMに接続するために RED アプライアンスを有効にするには、次の手順に従います。

1. **「*クライアントマネジメント*」タブで、「*RED の追加*」をクリックします。**
   「*RED の追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
ブランチ名:RED アプライアンスが配置されたブランチ名を入力します(例:「ミュンヘンオフィス」)。

クライアント種別:接続する RED アプライアンスの種別に応じて、ドロップダウンリストから *RED 10* か *RED 50* を選択します。

RED ID:設定している RED アプライアンスの ID を入力します。この ID は、RED アプライアンスの背面とパッケージに記載されています。

トンネル ID:デフォルトでは「*自動*」が選択されています。トンネルには順番に番号が付けられます。ID が重複する場合は、ドロップダウンリストから別の ID を選択します。

ロック解除コード(オプション):はじめて RED アプライアンスを導入する場合は、このボックスは空欄のままにしておきます。設定中の RED アプライアンスを以前に導入したことがある場合は、ロック解除コードを指定する必要があります。ロック解除コードは、RED アプライアンスの導入時に生成され、「*グローバル設定*」タブで設定したアドレス宛てにすぐにメール送信されます。これはセキュリティ機能であり、RED アプライアンスを簡単に切断してどこにでもインストールできなくなります。

注 – USB メモリでの手動インストールおよび RED プロビジョニングサービス(以下参照)による自動インストールについては、2つのロック解除コードが生成されます。RED デバイスのインストール方法を別の方法に変更する場合は、必ず対応するロック解除コードを使用してください。手動インストールの場合、前回の手動インストール時のロック解除コードを指定します。自動インストールの場合、前回の自動インストール時のロック解除コードを指定します。

(ロック解除コードを紛失した場合、RED アプライアンスをロック解除するためには、Sophos サポートに連絡してください。)ただし、サポートが対応できるのは Sophos RED プロビジョニングサービスによって設定を自動でインストールした場合に限ります。

ヒント – バックアップファイルにホスト固有のデータが含まれる場合は、ロック解除コードは、RED が接続されていた UTM のバックアップファイルの中にも保存されています。

UTM ホスト名:UTMがアクセスできるパブリック IP アドレスまたはホスト名を入力する必要があります。

2台目の UTM ホスト名:RED 50 アプライアンス用に同じUTMの別のパブリック IP アドレスまたはホスト名を入力することができます。注一異なる IP アドレスもしくはホスト名を入力することはできませんUTM。

第 2 ホスト名の用途:(RED 50 のみ。下図参照):第 2 ホスト名の使用目的を設定できます。

- **フェイルオーバ:**1台目のホスト名に障害が発生した場合にのみ第 2 ホスト名を使用する場合に選択します。
- **分散:**2つのホスト名間の負荷分散を有効にする場合に選択します。1台目のホスト名と2台目のホスト名に関連付けられたアップリンクが両方とも同程度の待ち時間とスループットである場合に効果があります。

アップリンクモード/2つ目のアップリンクモード:DHCP 経由か直接スタティック IP を設定するのか、RED アプライアンスの IP アドレス取得方法を定義できます。RED 50 アプライアンスではそれぞれのイーサネットポートに対しアップリンクモードを定義することができます。

- **DHCP クライアント:**RED は DHCP サーバから IP アドレスを取得します。
- **スタティックアドレス:**IPv4 アドレス、関連するネットマスク、デフォルトゲートウェイ、DNS サーバを入力します。

注 – ホスト名と RED のアップリンクイーサネットポートのUTM 1対1の関連性はありません。それぞれの RED のポートはそれぞれに定義されたに対し接続を試みます。UTM そして

第 2 アップリンクの除外:(RED 50 のみ。下図参照):第 2 アップリンクの使用目的を設定できます。

- **フェイルオーバ:**1台目のアップリンクに障害が発生した場合にのみ第 2 アップリンクを使用する場合に選択します。
- **分散:**2つのアップリンク間の負荷分散を有効にする場合に選択します。RED 50 アプライアンスの 2つのアップリンクの待ち時間とスループットが同程度である場合に効果があります。

オペレーションモード:リモートネットワークのローカルネットワークへの統合方法を定義できます。

- **標準/統合:**UTMがリモートネットワークのネットワークトラフィックを完全にコントロールします。さらに、DHCP サーバおよびデフォルトゲートウェイとして機能します。全てのリモートネットワークはを経由しますUTM.

- **標準/分割:**UTMがリモートネットワークのネットワークトラフィックを完全にコントロールします。さらに、DHCP サーバおよびデフォルトゲートウェイとして機能します。さらに、1つ以上のUTM分割ドメインをアクセス可能として定義することができます。下の「*分割ネットワーク*」ボックスに、リモートクライアントからアクセス可能なローカルネットワークを定義します。

  注 – VLAN タグの付いたフレームは、この操作モードでは処理できません。RED アプライアンスの背後で VLAN を使用している場合合は、代わりに「*標準*」モードを使用してください。

- **透過/分割:**UTMは リモートネットワークのネットワークトラフィックをコントロールせず、DHCP サーバとしてもデフォルトゲートウェイとしても機能しません。代わりに、リモートネットワークの DHCPサーバから IP アドレスを取得して、ネットワークの一部とします。ただし、リモートクライアントからローカルネットワークへのアクセスは有効化することができます。そのために、リモートネットワークによるアクセスを許可する*分割ネットワーク*を定義する必要があります。さらに、1つ以上の *分割ドメイン*をアクセス可能として定義することができます。ローカルドメインがパブリックに解決可能ではない場合、リモートクライアントからクエリ(問い合わせ)可能な*分割 DNS サーバ*を定義する必要があります。

  注 – VLAN タグの付いたフレームは、この操作モードでは処理できません。RED アプライアンスの背後で VLAN を使用している場合合は、代わりに「*標準*」モードを使用してください。

すべてのオペレーションモードの例は、「*導入ヘッダ*」タブで参照できます。

3. **次の詳細設定を任意で行います。**

MAC フィルタリングタイプ:この RED アプライアンスへの接続が許可される MAC アドレスを制限するには、「*ブラックリスト*」または「*ホワイトリスト*」を選択します。*ブラックリスト*を使用する場合、以下の MAC アドレスリストで指定したものを除く、すべての MAC アドレスが許可されます。*ホワイトリスト*を使用する場合、以下の MAC アドレスリストで指定したものを除く、すべての MAC アドレスがブロックされます。

MAC アドレス:RED アプライアンスへのアクセスを制限するために使用する MAC アドレスのリスト。MAC アドレスのリストは、「*定義とユーザ > ネットワーク定義 > MAC アドレス定義*」タブで作成できます。

デバイスの導入:RED の設定に必要な構成を導入する方法を選択します。デフォルトで、UTM は RED の設定データを Sophos の RED プロビジョニングサービスによって自動で設定します。この場合、RED アプライアンスはインターネット経由で設定を受信します。RED がインターネットに接続していない場合は、USB メモリにより手動で設定を導入できます。

注 – 手動によるデバイスの導入は、ファームウェアのバージョンが 9.1 以降の RED アプライアンスのみで実行できます。

警告 – 手動による導入を選択する場合は、特に、メールで送信されるロック解除コードをなくさずに保管しておく必要があります。ロック解除コードを紛失した場合、RED アプライアンスを他の UTM と接続することが出来なくなります。

3G/UMTS フェイルオーバ:RED リビジョン 2 以降では、RED アプライアンスに USB ポートが付いているため、3G/UMTS USB メモリを接続できます。これを選択すると、WAN インタフェースに障害が発生した際、このメモリはインターネットアップリンクのフェイルオーバーとして機能します。必要な設定については、インターネットプロバイダーの設定ガイドを参照してください。

- **ユーザ名/パスワード**(任意):必要な場合、モバイルネットワークのユーザ名とパスワードを入力します。
- **PIN**(任意):PIN が設定されている場合、SIM カードの PIN を入力します。

  注 – 間違った PIN を入力すると、WAN インタフェースの障害時に、3G/UMTS による接続が確立できません。その場合、RED アプライアンスの「*3G/UMTS フェイルオーバー*」チェックボックスは自動的に選択が解除されます。これにより、間違った PIN は一度しか使用されません。WAN インタフェースが復旧すると、RED アプライアンスに警告が表示されます。*3G/UMTS フェイルオーバーのアップリンクに間違った PIN が入力されました。ログイン情報を変更してください。*「*RED の編集*」ダイアログボックスを開くと、*3G/UMTS フェイルオーバー*が自動的に選択解除されたことを示すメッセージが表示されます。チェックボックスを再度選択する前に、PIN を修正してください。間違った PIN で3回接続を試行すると、SIM カードはロックされます。ロックの解除は RED アプライアンスや UTMではできません。

- **モバイルネットワーク:**モバイルネットワークの種類を、GSM または CDMA から選択します。
- **APN:**プロバイダのアクセスポイント名の情報を入力します。

- **ダイヤル文字列**(オプション):プロバイダが異なるダイヤル文字列を使用している場合、ここに入力します。デフォルトは *99# です。

注 – 次の設定は必ず手動で行ってください。1) 必要なファイアウォールルールの作成(「*ネットワークプロテクション > ファイアウォール > ルール*」)。2) 必要なマスカレードルールの作成(「*ネットワークプロテクション > NAT > マスカレード*」)。

4. **「*保存*」をクリックします。**
   RED アプライアンスが作成され、「*RED*」リストに表示されます。

自動によるデバイスの導入では、RED の起動直後に、SophosRED プロビジョニングサービス(RPS)から設定が取得されます。その後、UTMとの接続 UTM REDアプライアンスが確立されます。

手動によるデバイスの導入では、「*RED*」リストの新しいエントリには「*ダウンロード*」ボタンが表示されます。設定ファイルをダウンロードし、USB メモリのルートディレクトリに保存します。次に、USB メモリを RED アプライアンスの電源を入れる前に差し込みます。RED は USB メモリから設定を取得します。その後、UTM との接続 UTM RED アプライアンスが確立されます。

警告 –ロック解除コードを必ず保管しておいてください。ロック解除コードは、RED アプライアンスが設定を受信した後すぐに「*グローバル設定*」タブで指定したアドレスにメールで送信されます。(手動と自動の導入を切り替えた場合は、それぞれのロック解除コードを必ず保管しておいてください。)このロック解除コードは、他で RED アプライアンスを使用するときに必要になります UTM. ロック解除コードが手元にない場合、RED アプライアンスをロック解除するためには、Sophosサポートに連絡する必要があります。ただし、サポートが対応できるのは Sophos RED プロビジョニングサービスによって設定を自動でインストールした場合に限ります。

RED アプライアンスを編集するには、対応するボタンをクリックします。設定されたすべての RED アプライアンスのステータスは、WebAdmin の *RED* 概要ページで確認できます。

下図は、RED 50 で提供する分散/フェイルオーバーの4つの組み合わせを示しています。実線は分散を表し、点線はフェイルオーバーを表しています。

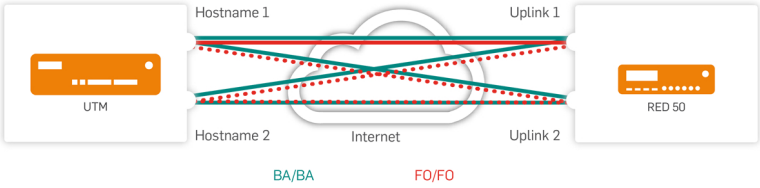

Figure 25 RED 50:ホスト名とアップリンクとも分散(青緑)およびホスト名とアップリンクともフェイルオーバー(赤)

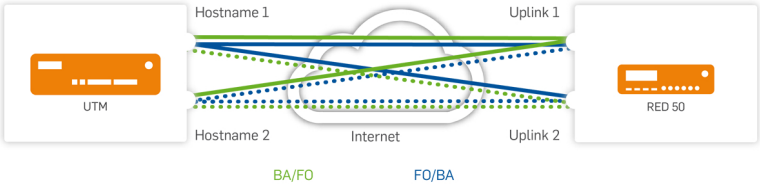

Figure 26 RED 50:ホスト名の分散とアップリンクのフェイルオーバー(緑)およびホスト名のフェイルオーバーとアップリンクの分散(青)

RED アプライアンスの削除

RED アプライアンスを削除するには、アプライアンス名の横にある「*削除*」ボタンをクリックします。RED オブジェクトに依存関係があるという警告が表示されます。RED アプライアンスを削除しても、関連するインタフェースと依存関係は*削除されません*。これは、RED アプライアンス間でインタフェースを移動できるようにするための意図的な設計です。

RED アプライアンスの設定を完全に削除するには、潜在的なインタフェースとその他の定義を手動で削除してください。

14.4 [サーバ] 導入ヘルパ

「*RED マネジメント > 導入ヘルパ*」タブには、RED 環境のセットアップと統合のためのウィザードがあります。このウィザードは、「*クライアントマネジメント*」タブでの通常の設定の簡易版となります。必須フィールドと、必要に応じて「*オプション*」マークの付いたフィールドに入力して、「*RED の導入*」をクリックするだけです。

ページ名の前に *[サーバ]* タグが付いている場合は、UTMをサーバ(RED ハブ)として機能させる場合にのみ、このページの設定が必要になることを表しています。

注 – 利便性のため、「*標準*」および「*標準/分割*」モードでは、「*クライアントマネジメント*」タブと違い、導入ヘルパが指定した IP アドレスのローカルインタフェース、利用可能な IP アドレス範囲の半分をカバーするリモートネットワーク用 DHCP サーバ、ローカル DNS リゾルバへのアクセスといったオブジェクトを自動的に作成します。「*透過/分割*」モードでは、導入ヘルパは DHCP クライアント（*イーサネット DHCP*）インタフェースのみ作成します。

導入ヘルパは、各オプションについて概要を提供し、RED テクノロジーで提供される 3つのオペレーションモードそれぞれについてスケッチを提供します。

以下は、RED の 3つのオペレーションモードの説明と使用例です。

標準

UTMがリモートネットワーク全体を管理します。DHCP サーバおよびデフォルトゲートウェイとして機能します。

例:支店が 1つあり、セキュリティ上の理由から、そのすべてのトラフィックを本店のUTM経由でルーティングしたい。これにより、リモートサイトは、LAN 経由で接続されているようにローカルネットワークの一部となります。

標準/分割

注 – VLAN タグの付いたフレームは、この操作モードでは処理できません。RED アプライアンスの背後で VLAN を使用している場合合は、代わりに「*標準*」モードを使用してください。

「*標準*」モードと同様に、UTMがリモートネットワーク全体を管理します。DHCP サーバおよびデフォルトゲートウェイとして機能します。ただし、「*分割ネットワーク*」ボックスにリストされたネットワーク宛てのトラフィックのみが、ローカルUTMにリダイレクトされる点が異なります。定義された分割ネットワークから発生していないすべてのトラフィックは、インターネットに直接ルーティングされます。

例:支店が 1つあり、セキュリティ上の理由から、ローカルイントラネットへのアクセスを必要としているか、リモートネットワークのトラフィックをUTM経由でルーティングしたい（例えば、トラフィックに対するウイルスチェックのため、あるいは HTTP プロキシを使用するため）。

透過/分割

注 – VLAN タグの付いたフレームは、この操作モードでは処理できません。RED アプライアンスの背後で VLAN を使用している場合合は、代わりに「*標準*」モードを使用してください。

リモートネットワークは独立したままで、UTMは IP アドレスをリモートDHCP サーバから取得してこのネットワークの一部となります。リモートネットワークの特定のトラフィックのみ、特定のネットワークまたはローカルドメインへのアクセスが許可されます。UTMはリモートネットワークをコントロールできないため、*分割 DNS サーバ*を定義しない限り、パブリックに解決可能ではないローカルドメインをリモートルータで解決することはできません。これは、リモートクライアントからクエリ（問い合わせ）可能なローカル DNS サーバです。

技術的には、RED アプライアンスのローカルインタフェースと、ローカルのUTMへのアップリンクインタフェース、並びにリモートルータへのリンクは、このモードでブリッジされます。（RED 50 アプライアンスでは、LAN ポートは WAN 1 にしかブリッジされません。）UTMはリモートネットワークの唯一のクライアントであるため、分割ネットワークへのトラフィックを他のモードと同様にルーティングすることはできません。そのため、RED アプライアンスはすべてのトラフィックをインターセプトします。「*分割ネットワーク*」ボックスにリストされたネットワーク宛てのトラフィックや、「*分割ドメイン*」ボックスにリストされたドメイン宛てのトラフィックは、UTMインタフェースにリダイレクトされます。これは、各データパケット内でデフォルトゲートウェイの MAC アドレスをUTMの MAC アドレスに置き換えることで実現します。

例:イントラネットや、ローカルネットワーク内の特定のサーバへのアクセスが必要なパートナーまたはサービスプロバイダがいる。RED アプライアンスを使用することで、このパートナーのネットワークは自社のネットワークからの独立が完全に保たれますが、特定の目的のために、自社のネットワークの決められた部分に LAN 経由で接続しているかのようにアクセスすることはできます。

注 – 導入ヘルパを使用すると、RED アプライアンスのアップリンクモードはいずれのオペレーションモードでも*DHCP クライアント*となります。代わりにスタティック IP アドレスを割り当てる必要がある場合は、「*クライアントマネジメント*」タブで RED アプライアンスを設定する必要があります。

14.5 [クライアント] トンネルマネジメント

「*RED マネジメント > トンネルマネジメント*」ページでは、別のUTMに REDトンネルを確立するために、UTMを RED アプライアンスとして機能するように設定できます。これにより、リモートホストUTMがUTMの RED ハブとして機能するようになります。

ページ名の前に *[クライアント]* タグが付いている場合は、UTMを RED クライアントとして機能させる場合にのみ、このページの設定が必要になることを表しています。

UTMをホストUTMに接続するためには、プロビジョニングファイルが必要になります。このファイルはホストUTMで作成する必要があります(「クライアントマネジメント」を参照)。

UTMをホストUTMに接続するには、次の手順に従います。

1. **ホストUTMで、ローカルUTMを「クライアントマネジメント」リストに追加します。**
2. **ホストUTMで、UTMプロビジョニングファイルをダウンロードします。**
3. **ローカルUTMで「*トンネルを追加*」をクリックします。**
   「*トンネルの追加*」ダイアログボックスが開きます。
4. **次の設定を行います。**
   トンネル名:このトンネルを説明する名前を入力します。

   UTM ホスト名:リモート UTM ホストを選択します。

   Prov.ファイル:フォルダアイコンをクリックし、アップロードするプロビジョニングファイルを選択して、「*アップロード開始*」をクリックします。

   コメント(任意):説明などの情報を追加します。
5. **「*保存*」をクリックします。**
   RED トンネルが確立され、「*トンネル マネジメント*」リストに表示されます。

15 サイト間 VPN

この章ではSophos UTMのサイト間 VPN 設定の構成方法について説明します。Sophos UTM のサイト間 VPN は、*バーチャルプライベートネットワーク*(VPN)によって実現します。VPN はインターネットなどのパブリックネットワーク上でリモートネットワークが機密性を保ち相互通信するためのセキュアでコスト効果の高い方法です。VPN では暗号化トンネリングプロトコルの IPsec を使用して、VPN 上を伝送されるデータの機密性とプライバシーを保ちます。

参照 – サイト間 VPN 接続の設定方法の詳細は、Sophos サポートデータベースを参照してください。

この章では、次のトピックについて説明します。

- Amazon VPC
- IPsec
- SSL
- 証明書管理

WebAdmin の「*サイト間 VPN*」概要ページには、設定されたすべての Amazon VPC、IPsec、および SSL コネクションとその現在のステータスが表示されます。各コネクションの状態は、そのステータスアイコンの色で示されます。ステータスアイコンは 2種類あります。コネクション名の隣りの大きなアイコンは、コネクションの全体的な状態を表します。それぞれの色は以下の状態を意味します。

- 緑色 – すべての SA (*セキュリティアソシエーション*) が確立されました。コネクションは完全に機能しています。
- 黄色 – SA の一部が確立されていません。コネクションは部分的に機能しています。
- 赤色 – SA がまったく確立されていません。コネクションが機能していません。

トンネル情報の隣りの小さなアイコンは、トンネルの状態を表します。それぞれの色は以下の状態を意味します。

- 緑色 – すべてのSA が確立されました。トンネルは完全に機能しています。
- 黄色 – IPsec SA が確立されましたが、ISAKMP SA (*インターネットセキュリティアソシエーションと鍵管理プロトコル*) が機能していません。トンネルは完全に機能しています。
- 赤色 – SA がまったく確立されていません。コネクションが機能していません。

15.1 Amazon VPC

Amazon VPC（バーチャルプライベートクラウド）は、商用クラウドコンピューティングサービスです。ユーザはバーチャルプライベートクラウドを作成した後、これをローカルネットワークに接続して、IPsecトンネルで集中管理することができます。

Sophos UTMにスタティックのパブリック IP アドレスがある場合は、Amazon VPC をUTMに接続できます。VPN コネクションのすべての設定は、Amazon 環境で行う必要があります。その後は、Amazon アクセスデータまたは設定ファイルを使用してコネクションデータをインポートするだけで済みます。

15.1.1 ステータス

「*サイト間 VPN > Amazon VPC > ステータス*」ページには、Amazon VPC のすべてのコネクションがリストされます。

ここでは、コネクションを有効または無効にすることができます。

Amazon VPC のコネクションを有効にするには、以下の手順に従います。

1. **「セットアップ」ページで、VPC 接続を 1つ以上インポートします。**
2. **「ステータス」ページで、Amazon VPC を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、インポートされた VPC 接続が表示されます。
3. **目的のコネクションを有効にします。**
   有効にするコネクションのトグルスイッチをクリックします。

   トグルスイッチが緑色になり、VPC コネクションの 2つのトンネルが表示されます。

   注 – 各コネクションは、冗長化のためにアクティブなトンネルとバックアップトンネルの 2つのトンネルから構成されます。アクティブなトンネルには、BGP 行の最後にネットマスクが表示されます。トンネルのステータスアイコンは制御目的のためにのみ表示されており、1つのトンネルを有効または無効にすることはできません。

すべての Amazon VPC コネクションを無効にするには、一番上のトグルスイッチをクリックします。1つのコネクションを無効にするには、そのコネクションのトグルスイッチをクリックします。

コネクションを閉じてリストから削除するには、そのコネクションの赤い削除アイコンをクリックします。

注 – コネクションは Amazon VPC 側で設定されているため、以前と同じデータを使用することで削除したコネクションをSophos UTMに再度インポートできます。

15.1.2 セットアップ

「*サイト間 VPN > Amazon VPC > セットアップ*」ページでは、Amazon VPC（バーチャルプライベートクラウド）に対するコネクションを追加できます。1つの Amazon Web Service（AWS）アカウントと、Sophos UTMの IP アドレスを*カスタマゲートウェイ*（VPC VPN 接続のエンドポイントを指す Amazon の用語）として使用して設定されているすべてのコネクションをインポートするか、Amazon からダウンロードできる設定ファイルを使用して 1つずつコネクションを追加できます。

Amazon クレデンシャルによるインポート

1つの AWS アカウントで設定したコネクションと、Sophos UTMの IP アドレスをカスタマゲートウェイとして使用して設定したコネクションをすべて一度にインポートすることができます。これには、単に Amazon Web Service アカウントの作成時に提供された AWS のクレデンシャルを入力します。

注 –「ステータス」タブにリストされた既存の全コネクションは、インポート中に削除されます。

コネクションをインポートするには、以下の手順に従います。

1. **次の設定を行います。**
   アクセスキー: Amazon アクセスキー ID を入力します。これは 20文字の英数字シーケンスです。

   シークレットキー:シークレットアクセスキーを入力します。これは 40文字のシーケンスです。

2. **「*適用*」をクリックします。**

   コネクションがインポートされ、「ステータス」ページに表示されます。

Amazon VPC 設定によるインポート

既存のコネクションリストに1つの接続を追加するには、そのコネクションの設定ファイルをアップロードする必要があります。

1つのコネクションをインポートするには、以下の手順に従います。

1. **Amazon VPC コネクションの設定ファイルをダウンロードします。**
   Amazon のダウンロードダイアログで、「ベンダー」ドロップダウンリストから「*Sophos*」を選択します。
2. **「*ファイルのアップロード*」ダイアログボックスを開きます。**
   「*VPC 設定ファイル*」ボックスの横にあるフォルダアイコンをクリックします。
3. **設定ファイルを選択してアップロードします。**
   選択したファイルをアップロードするには、「*アップロード開始*」ボタンをクリックします。

   ファイル名が「*VPC 設定ファイル*」ボックスに表示されます。
4. **スタティックルーティングを使用する場合は、リモートネットワークを入力してください。**
   リモートネットワークは、設定ファイルの一部ではありません。したがって、「*リモートネットワーク*」フィールドに、10.0.0.0/8 など別に入力する必要があります。このフィールドは、Amazon VPC で動的ルーティングでなく、静的ルーティングを使用するように設定した場合のみに重要です。
5. **「*適用*」をクリックします。**
   コネクションがインポートされ、「*ステータス*」ページに表示されます。

15.2 IPsec

IPsec (IP Security) とは、すべての IP パケットを暗号化または認証すること（あるいはその両方）によって IP *(インターネットプロトコル)* 通信のセキュリティを維持するための標準です。

IPsec 標準は、次の 2つのサービスモードと2つのプロトコルを定義しています。

- トランスポートモード
- トンネルモード
- *AH (認証ヘッダ)* 認証プロトコル
- *ESP (カプセル化セキュリティペイロード)* 暗号化（および認証）プロトコル

IPsec には、SA *(セキュリティアソシエーション)* と鍵配布を手動および自動で管理するための方法も用意されています。これらの特徴は、DOI *(解釈ドメイン)* で一元管理されています。

IPsec モード

IPsec は、トランスポートモードまたはトンネルモードで機能します。原則的に、ホスト間接続ではどちらのモードも使用できます。ただし、いずれかのエンドポイントがセキュリティゲートウェイである

場合、トンネルモードを使用する必要があります。この UTM での IPsec VPN 接続では、常にトンネルモードが使用されます。

トランスポートモードでは、元の IP パケットは他のパケットにカプセル化されません。元の IP ヘッダは維持され、パケットの残りの部分は平文のまま（AH）またはカプセル化されて（ESP）送信されます。パケット全体を AH で認証することも、ESP でペイロードをカプセル化して認証することもできます。いずれの場合も、元のヘッダは平文として WAN 経由で送信されます。

トンネルモードでは、パケットヘッダとペイロードの全体が新しい IP パケットにカプセル化されます。IP ヘッダが IP パケットに追加され、宛先アドレスは受信側トンネルエンドポイントに設定されます。カプセル化パケットの IP アドレスは変更なしで維持されます。続いて、元のパケットが AH で認証されるか、ESP でカプセル化されて認証されます。

IPsec プロトコル

IPsec では、IP レベルで安全に通信するために 2つのプロトコルを使用します。

- **AH（認証ヘッダ）:**パケット送信者を認証し、パケットデータの完全性を保証するためのプロトコル。
- **カプセル化セキュリティペイロード（ESP）:**パケット全体を暗号化し、そのコンテンツを認証するためのプロトコル。

AH *（認証ヘッダ）*プロトコルは、パケットデータの信頼性と完全性をチェックします。さらに、送信者と受信者の IP アドレスが送信中に変更されていないことをチェックします。パケットは、ハッシュベースの*メッセージ認証コード*（HMAC）と鍵を使用して作成されたチェックサムを使用して認証されます。次のいずれかのハッシュアルゴリズムが使用されます。

- **MD5（メッセージダイジェスト、バージョン 5）:**このアルゴリズムでは、任意のサイズのメッセージから 128ビットのチェックサムが生成されます。このチェックサムはメッセージの指紋のようなもので、メッセージが変更されるとチェックサムも変わります。このハッシュ値は、デジタル署名またはメッセージダイジェストとも呼ばれます。
- **SHA-1（セキュアハッシュ）:**このアルゴリズムでは MD5 と類似したハッシュが生成されますが、SHA-1 ハッシュは長さが 160ビットです。SHA-1 は鍵が MD5 より長いため、MD5 より強力なセキュリティが実現します。

MD5 と比較すると、SHA-1 ハッシュは計算が難しく、生成に必要な CPU 時間はより長くなります。もちろん、計算速度は、プロセッサの処理速度とSophos UTMで使用されるIPsec VPN 接続の数に依存します。

ESP *（カプセル化セキュリティペイロード）*プロトコルには、暗号化以外に、送信者を認証し、パケットコンテンツを検証する機能もあります。トンネルモードで ESP を使用すると、IP パケット全体（ヘッダ

とペイロード）が暗号化されます。ここで、暗号化されていない IP ヘッダと ESP ヘッダがカプセル化するパケットに追加されます。新しい IP ヘッダには、受信側ゲートウェイと送信側ゲートウェイのアドレスが含まれています。これらの IP アドレスは、VPN トンネルのアドレスです。

暗号化付きの ESP では、通常次のアルゴリズムが使用されます。

- 3DES（トリプルデータ暗号化標準）
- AES（高度暗号化標準）

これらのうち、AES が最も安全です。AES で使用可能な鍵の有効長は 128ビット、192ビット、256 ビットです。Sophos UTMSophos UTM は、多数の暗号化アルゴリズムをサポートしています。認証には MD5 または SHA-1 アルゴリズムを使用できます。

NATトラバーサル（NAT-T）

NAT トラバーサルとは、NAT デバイスを使用する TCP/IP ネットワーク内のホスト間で接続を確立するための技術です。この接続は、ESP パケットの UDP カプセル化を使用して、NAT デバイス経由で IPsec トンネルを確立することによって実現します。UDP カプセル化は、IPsec ピア間で NAT が検出された場合のみに使用されます。検出されなかった場合は、通常の ESP パケットが使用されます。

NAT トラバーサルにより、ゲートウェイまたはロードウォリアを NAT ルータの背後に配置しながら、IPsec トンネルを確立できるようになります。この機能を使用する場合、両方の IPsec ピアで NAT トラバーサルがサポートされている必要があります。ネゴシエーションは自動的に行われます。NAT デバイスで IPsec パススルーがオフになっていることを確認してください。オンになっていると、NAT トラバーサルの使用に支障が出る可能性があります。

ロードウォリアで NAT トラバーサルを使用する場合、WebAdmin 内の対応ユーザオブジェクトに静的なリモートアクセス IP アドレス（RAS アドレス）が設定されている必要があります（WebAdmin の「ユーザ」ページの「*リモートアクセスにスタティック IP アドレスを使用*」も参照してください）。

データ未送信時に確立されたトンネルが期限切れになることを防ぐために、NAT トラバーサルの keep-alive 信号がデフォルトで 60秒間隔で送信されます。keep-alive メッセージは、NAT ルータがセッションに関連するステート情報を維持しており、トンネルが開いたままであることを確認するために送信されます。

TOS

「サービスタイプ」ビット（TOS ビット）は、IP ヘッダにあるいくつかの 4ビットフラグです。これらのビットは、どのタイプのサービス品質が必要であるかを転送アプリケーションがネットワークに伝えるこ

とを許可するため、*サービスタイプビット*と呼ばれています。

Sophos UTMへの IPsec 導入では、TOS の値は常にコピーされます。

15.2.1 コネクション

「*サイト間 VPN > IPsec > コネクション*」タブでは、IPsec コネクションを作成および編集することができます。

IPsec コネクションを作成するには、次の手順に従います。

1. **「コネクション」タブで「*新規 IPsec コネクション*」をクリックします。**
   「*IPsec コネクションの追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:この接続を説明する名前を入力してください。

   リモートゲートウェイ:リモートゲートウェイ定義を選択します。リモートゲートウェイは、「*サイト間 VPN > IPsec > リモートゲートウェイ*」タブで設定します。

   ローカルインタフェース:IPsecトンネルのローカルエンドポイントとして使用されるインタフェースの名前を選択します。

   ポリシー:この IPsec コネクションの IPsec ポリシーを選択します。IPsec ポリシーは、「*サイト間 VPN > IPsec > ポリシー*」タブで定義できます。

   ローカルネットワーク:VPN トンネル経由でアクセス可能にするローカルネットワークを選択します。

   自動ファイアウォールルール:このオプションを選択すると、この接続用のトラフィックを許可するファイアウォールルールを自動的に追加することができます。ルールは、接続が確立するとすぐに追加され、接続が無効になると削除されます。より厳格な IPsec 接続を使用する場合は、「*自動ファイアウォールルール*」を無効にして、代わりにファイアウォールルールセット内の IPsec オブジェクトを使用してください。

   厳密ルーティング:ストリクトルーティングを選択すると、VPN ルーティングは（宛先 IP アドレスのみではなく）送信元 IP アドレスと宛先 IP アドレスに従って実行されます。この場合、VPN トンネル定義と完全に一致するパケットのみが VPN トンネルにルーティングされます。この結果、SNAT を使用して本来トンネル定義の一部ではないネットワークまたはホストを VPN トンネルに追加することはできません。一方、厳密ルーティングを使用しない場合、異なる送信元アドレスから同じネットワークに対して非暗号化/暗号化の混在するセットアップを行うことはできません。

トンネルをローカルインタフェースにバインド:デフォルトでこのオプションは選択解除されており、送信元が指定したローカルネットワークで、送信先が指定したリモートネットワークのトラフィックすべては、常に、この IPsec トンネル経由で送信されます。セレクタが常に同じであるため、異なるインターフェースに、同一のトンネルを複数バインドすることはできません。しかし、有効にした場合、指定した IPsec セレクタは、選択したローカルインターフェースにバインドされます。したがって、静的ルートで IPsec ポリシーを回避したり、異なるアップリンクを使用して冗長の IPsec トンネルを指定して、マルチパスルールを使用して、使用可能なインターフェースと IPsec トンネルにて、トラフィックの分散を実現することが可能です。この設定は次のような場合に使用します。

- スタティックルート経由でリモートネットワークに所属するローカルホストの IPsec ポリシーを回避する。
- マルチパスルールを使用したレイヤー 3 およびレイヤー 4 に基づいたトラフィックを、複数の IPsec トンネルや自動フェイルオーバーのある MPLS リンクで分散する。

注 – このオプションは、インターフェースグループでは使用できません。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しいコネクションが IPsec の「*コネクション*」リストに表示されます。

接続を編集または削除するには、対応するボタンをクリックします。

ライブログを開く:IPsec VPN ライブログには、確立された IPsec コネクションに関するモニタリング情報が表示されます。ボタンをクリックして、新しいウィンドウでライブログを開きます。

15.2.2 リモートゲートウェイ

「*サイト間 VPN > IPsec > リモートゲートウェイ*」タブでは、サイト間 VPN トンネル用にリモートゲートウェイを定義できます。これらのリモートネットワーク定義は、「*IPsec > コネクション*」タブで IPsec コネクションを作成すると使用可能になります。

リモートゲートウェイを追加するには、次の手順に従ってください。

1. **「*リモートゲートウェイ*」タブで、「*新規リモートゲートウェイ*」をクリックします。**
   「*リモートゲートウェイの追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このリモートゲートウェイを説明する名前を入力してください。

ゲートウェイタイプ:ゲートウェイのタイプを選択します。次のタイプを使用できます。

- **イニシエートを行う:**リモートエンドポイントに静的 IP アドレスがあり、リモートゲートウェイへの接続をゲートウェイによって開始できる場合に選択します。選択する場合、「*ゲートウェイ*」ボックスにリモートゲートウェイを指定します。このオプションは、リモートゲートウェイが DynDNS によって解決される場合にも選択できます。
- **レスポンドのみ:**リモートエンドポイントの IP アドレスが不明であるか、DynDNS で解決できない場合に選択します。ゲートウェイはリモートゲートウェイへの接続を開始できず、応答のみを行えば良い接続を受信するまで待機します。

認証タイプ:このリモートゲートウェイ定義の認証タイプを選択します。次のタイプを使用できます。

- **事前共有鍵:**「*事前共有鍵*」(PSK)による認証では、秘密のパスワードを鍵として使用します。これらのパスワードは、接続を確立する前にエンドポイントに配布する必要があります。新しい VPN トンネルが確立されると、両端で、相手側が秘密のパスワードを知っていることのチェックが行われます。PSK のセキュリティは、使用するパスワードの品質に依存します。一般的な言葉や成句では、辞書攻撃に対して脆弱です。常時の、または長期的な IPsec コネクションでは、パスワードの代わりに証明書を使用すべきです。
- **RSA 鍵:**RSA 鍵を使用する認証は、より高度です。この方式では、公開鍵と秘密鍵から成る鍵ペアが接続の両端で生成されます。秘密鍵は、鍵交換時の暗号化と認証で必要です。この認証方式を使用する IPsecVPN 接続の両エンドポイントは、独自の鍵ペアを必要とします。リモートユニットの公開 RSA 鍵(「*サイト間 VPN > IPsec > ローカル RSA 鍵*」)をローカルユニットの「*公開鍵*」ボックスにコピーし、逆方向のコピーも行います。さらに、それぞれの RSA 鍵に対応する VPN ID タイプと VPN 識別子を入力します。
- **ローカル X.509 証明書:**同様に、X.509 証明書による認証方式も公開鍵と秘密鍵を使用します。X.509 証明書には、公開鍵と、鍵の所有者を特定する情報が含まれています。このような証明書は、信頼される*認証局*(CA)によって署名され、発行されたものです。鍵交換中に証明書が交換され、ローカル保存された CA 証明書を使用して認証されます。リモートゲートウェイの X.509 証明書がユニットにローカル保存されている場合、この認証タイプを使用してください。
- **リモート X.509 証明書:**リモートゲートウェイの X.509 証明書がユニットにローカル保存されていない場合、この認証タイプを使用してください。リモートユニットで使用されている証明書の VPN ID タイプと VPN 識別子を選択する必要があります。この証明書は、「*サイト間 VPN > IPsec > 詳細*」タブの「*ローカル X.509 証明書*」エリアで選択されたものです。

VPN ID タイプ:認証タイプによっては、VPN ID タイプと VPN 識別子を選択する必要があります。ここで入力する VPN 識別子は、リモートサイトで設定した値と一致している必要があります。サイト間 VPN トンネルの確立に 2台のUTMアプライアンスを使用しているとします。ローカルユニットでの認証タイプとして「*RSA 鍵*」を選択する場合、VPN ID タイプと VPN 識別子がリモートユニットの「*サイト間 VPN > IPsec > ローカル RSA 鍵*」タブでの設定と一致している必要があります。次の VPN ID タイプを選択できます。

- **IP アドレス**
- **ホスト名**
- **メールアドレス**
- **識別名:***リモート X.509 証明書*認証のみで使用。
- **任意:**「*応答のみ*」ゲートウェイタイプのデフォルト。

リモートネットワーク:リモートゲートウェイ経由でアクセス可能にするリモートネットワークを選択します。

コメント(任意):説明などの情報を追加します。

3. **必要に応じて、詳細設定を行います。**
以下の詳細設定は、影響を理解している場合にのみ行ってください。

Path MTU ディスカバリのサポート:PMTU(パス最大伝送単位)とは、送信されるデータパケットのサイズです。IP データパケットは、送信元から宛先までのパスのどこでもフラグメンテーション(断片化)を必要としない最大サイズにすることが望まれます。パス上の一部ルータにとって断片化しないで転送するには大き過ぎるデータパケットがある場合、そのルータはそれらを破棄して、*ICMP Destination Unreachable* メッセージを「fragmentation needed and DF set」を意味するコードとともに返します。送信元ホストは、そのようなメッセージを受信すると、そのパスに対して想定される PMTU を減らします。
このオプションを有効にすると、サーバ側で PMTU が有効になっている場合にUTMが PMTU を有効化します。

輻輳状態通知サポート(ECN):ECN(明示的な輻輳通知)とはインターネットプロトコルの拡張であり、ネットワーク輻輳のエンドツーエンドな通知をパケットのドロップなしで許可します。元の IP パケットのヘッダから IPsec パケットのヘッダに ECN 情報をコピーするには、このオプションを選択します。リモートエンドポイントおよび下位のネットワークと関与するルータがこれをサポートしている必要があります。

XAUTHクライアントモードの有効化:XAUTHとは、IPsec IKE の拡張であり、VPN ゲートウェイでユーザ名とパスワードを使用してユーザを認証します。このリモートゲートウェイでの認証

に XAUTH を使用するためには、このオプションを選択して、リモートゲートウェイの要求に従ってユーザ名とパスワード(2回)を入力します。

4. **「*保存*」をクリックします。**
   ゲートウェイ定義が「*リモートゲートウェイ*」リストに表示されます。

リモートゲートウェイ定義を編集または削除するには、対応するボタンをクリックします。

15.2.3 ポリシー

「*IPsec > ポリシー*」タブでは、IPsec コネクション用のパラメータをカスタマイズし、ポリシーに統合することができます。IPsec ポリシーは、IPsec コネクションの IKE(インターネット鍵交換)と IPsec プロポーザルパラメータを定義します。それぞれの IPsec コネクションには IPsec ポリシーが必要です。

注 – Sophos UTM は、IKE フェーズ 1 のメインモードのみをサポートしています。アグレッシブモードはサポートされていません。

IPsec ポリシーを作成するには、以下の手順に従います。

1. **「*ポリシー*」タブで、「*新規 IPsec ポリシー*」をクリックします。**
   「*IPsec ポリシーの追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このポリシーを説明する名前を入力します。

   IKE 暗号化アルゴリズム:暗号化アルゴリズムでは、IKE メッセージの暗号化に使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。

   - *DES*(56ビット)
   - *3DES*(168ビット)
   - *AES 128*(128ビット)
   - *AES 192*(192ビット)
   - *AES 256*(256ビット)
   - *Blowfish*(128ビット)
   - *Twofish*(128ビット)
   - *Serpent*(128ビット)

セキュリティに関する注記 – DES の使用は推奨されません。アルゴリズムの強度が低いため、脆弱性につながる可能性があります。

IKE 認証アルゴリズム:認証アルゴリズムでは、IKE メッセージの完全性チェックに使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。

- *MD5*(128ビット)
- *SHA1*(160ビット)
- *SHA2 256*(256ビット)
- *SHA2 384*(384ビット)
- *SHA2 512*(512ビット)

IKE SA ライフタイム:この値には、IKE SA(セキュリティアソシエーション)が有効な期間(つまり次の鍵更新を行うタイミング)を秒単位で指定します。有効な値は 60秒～28800秒(8時間)です。デフォルト値は 7800秒です。

IKE DH グループ:接続をネゴシエートする際は、通信するパーティはデータの暗号化に使用する実際の鍵についても取り決めます。IKE はセッション鍵を生成するために、ランダムデータを利用する *Diffie–Hellman*(DH)アルゴリズムを使用します。ランダムデータの生成はプールビットに基づいて行われます。基本的には IKE グループがプールビット数を知らせます。プールビット数が多いほど、ランダムな数字が大きくなります。数字が大きいほど、Diffie–Hellman アルゴリズムの解読は難しくなります。結果として、プールビット数が多ければ安全ですが、CPU の使用量も増えます。現在は以下の Diffie–Hellman グループがサポートされています。

- *Group 1:MODP 768*
- Group 2:MODP 1024
- *Group 5:MODP 1536*
- *Group 14:MODP 2048*
- *Group 15:MODP 3072*
- *Group 16:MODP 4096*

セキュリティに関する注記 – グループ1(MODP 768)は弱く、相互運用性の理由のみからサポートされています。使用は推奨されません。脆弱性につながる可能性があります。

IPsec 暗号化アルゴリズム:IKE の場合と同じ暗号化アルゴリズム。さらに、以下のエントリもあります。

- *暗号化なし (null)*
- *AES 128 CTR* (128ビット)
- *AES 192 CTR* (192ビット)
- *AES 256 CTR* (256ビット)
- *AES 128 GCM (96ビット)*
- *AES 192 GCM (96ビット)*
- *AES 256 GCM (96ビット)*
- *AES 128 GCM (128ビット)*
- *AES 192 GCM (128ビット)*
- *AES 256 GCM (128ビット)*

セキュリティに関する注記 – 暗号化を実行しないこと、または DES の使用は推奨されません。脆弱性につながる可能性があります。

IPsec 認証アルゴリズム:IKE の場合と同じ認証アルゴリズム。さらに、以下のアルゴリズムもあります。

- *SHA2 256* (96ビット)
- *SHA2 384* (96ビット)
- *SHA2 512* (96ビット)

これらは、バージョン 8 より古い UTM (つまり ASG) など、RFC 4868 に準拠していないトンネルエンドポイント用です。切り捨てられたチェックサムで 96ビットより長いものには対応していません。

IPsec SA ライフタイム:この値には、IPsec SA が有効な期間 (つまり次の鍵更新を行うタイミング) を秒単位で指定します。有効な値は 60秒～86400秒 (1日) です。デフォルト値は 3600秒です。

IPsec PFS グループ: *Perfect Forward Secrecy* (PFS) という概念では、セッション鍵を使用できなくなった場合に、この特定セッションのデータにのみアクセスを許可します。PFS が存在するには、IPsec SA の保護に使用される鍵は、IKE SA の鍵を取得するために使用されるラ

ンダム鍵作成用のマテリアルから派生したものではないことが必要です。その場合、PFS は 2回目の Diffie-Hellman 鍵交換を開始し、IPsec 接続に対して選択された DH グループが新たにランダム生成された鍵を取得することを提案します。サポートされている Diffie-Hellman グループは IKE の場合と同じです。
PFS を有効にすると安全性が高まりますが、交換にさらに時間がかかるようになります。低速なハードウェアでは PFS は使用しないことをお勧めします。

注 – PFS はすべてのベンダーとの完全な相互運用性はありません。ネゴシエーション時に問題が発生したら、PFS を無効にしてください。

厳密ポリシー:IPsec ゲートウェイが暗号化アルゴリズムおよびその強度について提案を行うと、IPsec ポリシーがそれに対応していない場合でも、受信側ゲートウェイがこの提案を受け入れる場合があります。このオプションを選択すると、指定したパラメータを厳密にそのとおり使用することについてリモートエンドポイントが合意しないときは、IPsec 接続は確立されません。UTMの IPsec ポリシーが AES-256 暗号化を必要とする際に、SSH Sentinel を使用するロードウォリアが AES-128 を使用して接続しようとすると、厳格なポリシーオプションが有効である場合は、接続は拒否されます。

注 – 圧縮の設定は「*ストリクトポリシー*」を介しては施行されません。

圧縮:*IP ペイロード圧縮プロトコル*(IPComp)によってIPパケットを暗号化の前に圧縮するかどうかを指定します。IPComp は IP パケットを圧縮してそのサイズを縮小し、通信ホストまたはゲートウェイのペア間の全体的な通信パフォーマンスを向上させます。デフォルトでは圧縮はオフになっています。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しいポリシーが「*ポリシー*」リストに表示されます。

ポリシーを編集または削除するには、対応するボタンをクリックします。

15.2.4 ローカル RSA 鍵

RSA 認証では、VPN エンドポイントの認証に RSA 鍵が使用されます。エンドポイントの公開鍵は、コネクションが確立される前に手動で交換する必要があります。この認証タイプを使用する場合、VPN 識別子を定義して、ローカル RSA 鍵を作成する必要があります。ゲートウェイの公開

RSA 鍵を、Sophos UTM に対して IPsec RSA 認証を使用するリモート IPsec デバイスで使用できるようにする必要があります。

現在のローカル公開 RSA 鍵

現在インストールされているローカル RSA 鍵ペアの公開部分が表示されます。ボックスをクリックし、Ctrl-A と Ctrl-C を押してクリップボードにコピーしてください。

ローカル RSA 鍵 VPN オプション

お客様のニーズに最適な VPN ID タイプを選択します。デフォルトでは、ゲートウェイのホスト名が VPN 識別子として取得されます。スタティック(静的)IP アドレスをローカル VPN エンドポイントとする場合は、「*IP アドレス*」を選択します。あるいは、モバイル IPsec ロードウォリアの VPN ID としてメールアドレスを使用することもできます。

- **ホスト名:**デフォルト設定はゲートウェイのホスト名です。ただし、ここで他のホスト名を入力することもできます。
- **メールアドレス:**デフォルトではゲートウェイの admin アカウントのメールアドレスです。ただし、ここで他のメールアドレスを入力することもできます。
- **IP アドレス:**ゲートウェイの外部インタフェースの IP アドレス。

設定を保存するには「*適用*」をクリックします。設定を変更しても、RSA 鍵に変化はありません。

ローカル RSA 鍵の再生成

新しい RSA 鍵を生成するには、希望する鍵サイズを選択し、「*適用*」をクリックします。これにより、鍵生成プロセスが開始します。選択した鍵の長さと使用しているハードウェアに応じて、処理には数分から最大 2時間かかる場合があります。鍵サイズ(鍵の長さ)は、1つの暗号で使用可能な鍵の数の尺度です。長さは通常、ビットで指定します。次の鍵サイズがサポートされています。

- 1024 ビット
- 2048 ビット
- 4096 ビット

RSA 鍵を生成すると、適切な公開鍵が「*現在のローカル公開 RSA 鍵*」ボックスに表示されます。新しい RSA 鍵を生成すると、古い鍵が上書きされます。

15.2.5 詳細

「*サイト間 VPN > IPsec > 詳細*」タブでは、IPsecVPN の詳細オプションを設定することができます。希望の認証タイプに応じて、ローカル証明書 (X.509 認証の場合) やローカル RSA 鍵 (RSA 認証の

場合）などを定義可能です。この設定は熟練ユーザのみが行ってください。

ローカル X.509 証明書

X.509 認証では、証明書を使用して VPN エンドポイントの公開鍵を検証します。この認証タイプを使用する場合は、「*ローカル X.509 証明書*」エリアのドロップダウンリストからローカル証明書を選択する必要があります。選択した鍵/証明書は、X.509 認証が選択された場合のリモートピアへのゲートウェイの認証に使用されます。

適切な秘密鍵がある証明書のみ選択できます。他の証明書はこのドロップダウンリストでは利用できません。

選択できる証明書がない場合、新しい証明書を作成するか、またはアップロード機能を使用してインポートして、「*証明書管理*」メニューで追加する必要があります。

証明書を選択したら、秘密鍵を保護するパスフレーズを入力します。パスフレーズは保存プロセスで確認され、パスフレーズが暗号化鍵と一致しない場合はエラーメッセージが表示されます。

アクティブな鍵/証明書を選択すると、それは「*ローカル X.509 証明書*」エリアに表示されます。

デッドピア検出（DPD）

デッドピア検出（DPD）を使用デッドピア検出オプションを使用して、リモート VPN ゲートウェイあるいはクライアントに接続できない場合は接続を自動的に終了します。スタティックエンドポイントとの接続では、トンネルは自動的に再ネゴシエートされます。ダイナミックエンドポイントとの接続では、リモート側でトンネルの再ネゴシエートを行うことが必要です。通常はこのオプションを常に有効にしておくほうが安全です。IPsec ピアはリモート側がデッドピア検出をサポートするかどうかを自動的に判断し、必要に応じて通常モードにフォールバックします。

NAT トラバーサル（NAT-T）

NATトラバーサルを使用:このオプションを選択すると、IPsec トラフィックは、「*ネットワークアドレス変換*」(NAT)を使用するアップストリームシステムを通過できるようになります。さらに、NATトラバーサルのキープアライブ（keepalive）間隔を定義できます。 設定を保存するには「*適用*」をクリックします。

CRL処理

証明書のプロバイダが、まだ有効な証明書に与えられる承認を取り消す場合があるかもしれません。たとえば、証明書の受取人が不正なデータ(名前など)を使ってそれを不正に取得したことが判明した場合や、証明書に埋め込まれた公開鍵の一部である秘密鍵を攻撃者が入手した場合は、証明書が失効します。そのような場合に備えて、いわゆる*証明書失効リスト*(CRL)が使用されます。CRL には通常、依然として有効期間は残っているものの無効とされた証明書のシリアル番号が含まれています。
これらの有効期限が切れると、証明書は無効になり、ブロックリストから削除されます。

自動取得:この機能は、HTTP、Anonymous(匿名)FTP、または LDAP バージョン 3 を介しパートナー証明書で定義された URL を通して CRL を要求します。有効期限が切れたら、要求によって CRL をダウンロードし、保存して更新できます。この機能を、ポート80 または 443 を経由せずに使用する場合は、適切なファイアウォールルールを設定して、CRL 配布サーバにアクセスできるようにしてください。

厳密ポリシー:このオプションを有効にすると、対応する CRL のないパートナー証明書は拒否されます。

PSK プローブ:

応答のみモードを使用したIPsec接続では、それぞれの IPsec 接続に対して別々の事前共有鍵(PSK)を使用することを選択できます。

PSKプローブの有効化このチェックボックスにチェックを入れて、このオプションを有効にします。この設定は、L2TP-over-IPsec、リモートアクセス IPsec、VPN IPsec の各接続に影響を与えます。

15.2.6 デバッグ

IKEデバッグ

「*IKE デバッグ*」セクションで IKE デバッグオプションを設定できます。どのタイプの IKE メッセージまたは通信についてデバッグ出力を作成するかはチェックボックスで選択します。

注 – 「*IKE デバッグ*」セクションは、「*サイト間 VPN IPsec*」、「*リモートアクセス IPsec*」、「*L2TP over IPsec*」、および「*Cisco VPN クライアント*」メニューの「*デバッグ*」タブで同じものが使用されています。

以下のフラグをログできます。

- **コントロールフロー:**IKE ステートのコントロールメッセージを表示します。
- **アウトバウンドパケット:**送信 IKE メッセージのコンテンツを表示します。
- **インバウンドパケット:**受信 IKE メッセージのコンテンツを表示します。
- **カーネルメッセージ:**カーネルとの通信メッセージを表示します。
- **冗長構成 (HA)**その他の HA ノードとの通信を表示します。

15.3 SSL

サイト間 VPNトンネルは SSL 接続を介して確立できます。SSL VPN 接続には明確な役割があります。トンネルエンドポイントはクライアントまたはサーバとして機能します。常にクライアントが接続を開始し、サーバがクライアントの要求に応答します。これは、通常は両方のエンドポイントが接続を開始できる IPsec とは対照的です。

注 – コネクションの確立に問題がある場合は、Web フィルタが透過モードで動作して SSL スキャンが有効になっているかどうかを確認してください。Web フィルタが透過モードで動作して SSL スキャンが有効になっている場合は、VPN 接続のターゲットホストが「*透過モードスキップリスト*」(「*Web プロテクション* > *Web フィルタリング* > *詳細*」の下)に追加されていることを確認してください。

15.3.1 コネクション

SSLVPN サイト間トンネルを作成するには、最初にサーバ設定を作成することが必要です。クライアントの設定は、常に 2番目のステップで行います。

サーバ設定を作成するには、次の手順に従います。

1. **「コネクション」タブで、「*新規 SSL コネクション*」をクリックします。**
   「*SSL コネクションの追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   コネクションタイプ:ドロップダウンリストから「*Server*」(サーバ)を選択します。

   コネクション名:このコネクションを説明する名前を入力してください。

   スタティック仮想 IP アドレスを使用 (任意):このオプションは、IP アドレスプールとクライアントのネットワーク環境に互換性がない場合のみ選択してください。デフォルトで、クライアントには「*仮想 IP プール*」(「*設定*」タブで設定)にある IP アドレスが割り当てられます。まれに、そのような IP アドレスがクライアントホストですでに使用されている場合があります。そ

のような場合は、「*スタティックピア IP*」フィールドに適切な IP アドレスを入力します。この IP アドレスは、トンネルセットアップ時にクライアントに割り当てられます。

ローカルネットワーク:リモートからのアクセスを許可する 1つ以上のローカルネットワークを追加します。

リモートネットワーク:ローカルネットワークへの接続を許可する 1つ以上のリモートネットワークを追加します。

注 –「*ローカルネットワーク*」と「*リモートネットワーク*」の設定は、後でクライアントの設定をやり直さずに変更できます。

自動ファイアウォールルール（任意）:有効にすると、UTM は、アクセスするすべての SSL VPN クライアントに対し、選択されたローカルネットワークへのアクセスを自動的に許可します。

コメント（任意）:説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しいSSLサーバコネクションが「*コネクション*」リストに表示されます。
4. **設定ファイルをダウンロードします。**
   新しく作成した SSL サーバコネクションの行にある「*ダウンロード*」ボタンを使用して、この接続のクライアント設定ファイルをダウンロードします。

   設定ファイルの暗号化（任意）:セキュリティのために設定ファイルを暗号化することを推奨します。パスワードを 2回入力します。
   「*ピア設定のダウンロード*」をクリックしてファイルを保存します。
   このファイルは、クライアント側の管理者がトンネルのクライアントエンドポイントをセットアップする際に必要になります。

次のステップはクライアントの設定で、これはサーバ側ではなくクライアント側で行います。ダウンロードしたクライアント設定ファイルが手元にあることを確認してください。

クライアント設定を作成するには、以下の手順に従います。

1. **「*コネクション*」タブで、「*新規 SSL コネクション*」をクリックします。**
   「*SSL コネクションの追加*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   コネクションタイプ:ドロップダウンリストから「*Client*」(クライアント)を選択します。

   コネクション名:このコネクションを説明する名前を入力してください。

設定ファイル:フォルダアイコンをクリックし、クライアント設定ファイルを参照して、「*アップロード開始*」をクリックします。

パスワード(任意):ファイルが暗号化されている場合は、パスワードを入力します。

HTTP プロキシサーバを使用(任意):クライアントがプロキシの背後にある場合は、このチェックボックスにチェックを入れ、プロキシの設定を入力します。

プロキシ認証を使用(任意):プロキシに対するクライアントの認証が必要な場合は、このチェックボックスにチェックを入れ、ユーザ名とパスワードを入力します。

ピアホスト名を上書き(任意):サーバシステムの通常のホスト名(または DynDNS ホスト名)をクライアントホストで解決できない場合は、このチェックボックスにチェックを入れ、ホスト名をここに入力します。

自動ファイアウォールルール(任意):有効にすると、UTM は、トンネル化ローカルネットワークとトンネル化リモートネットワーク上のホスト間のトラフィックを自動的に許可します。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しい SSL VPN クライアントコネクションが「*コネクション*」リストに表示されます。

クライアントコネクションを編集または削除するには、対応するボタンをクリックします。

「*サイト間 VPN*」メニューをクリックすると、概要ページに SSL VPN コネクションのステータスが表示されます。コネクションが確立すると、ステータスアイコンが緑色に変わります。その後、トンネル両側の相互接続されたサブネットに関する情報も参照可能になります。

15.3.2 設定

「*SSL > 設定*」タブで、SSL VPN サーバ接続の基本設定を設定できます。

注 – このタブは「*サイト間 VPN > SSL*」および「*リモートアクセス > SSL*」で同じです。ここで加えた変更は、常に両方の SSL 設定に影響を与えます。

サーバ設定

SSLVPN 接続について以下の設定を行うことができます。

- **インタフェースアドレス:**デフォルトは「すべて」です。Web アプリケーションファイアウォールを使用する場合、サービスが SSL 接続をリスンするためのインタフェースアドレスを指定する必要があります。サイト間/リモートアクセス SSL 接続ハンドラと Web アプリケーションファイ

アウォールが受信 SSL 接続を識別できるようにするために、この設定が必要です。

- **プロトコル:**使用するプロトコルを選択します。*TCP* または *UDP* を選択できます。
- **ポート:**ポートを変更できます。デフォルトは `443` です。ポート `10443`、SUM ゲートウェイマネージャポート `4422`、または WebAdmin インタフェースが使用しているポートは使用できません。
- **ホスト名を上書き:**「*ホスト名を上書き*」ボックスの値は、クライアント VPN 接続のターゲットホスト名として使用され、デフォルトではゲートウェイのホスト名になります。システムの通常のホスト名（または DynDNS ホスト名）にこの名前でインターネットから到達できない場合のみ、デフォルトを変更します。

仮想 IP プール

プールネットワーク:これは、特定の IP 範囲から SSL クライアントに IP アドレスを配布するために使用される仮想 IP アドレスプールです。デフォルトでは、「*VPN プール (SSL)*」が選択されています。別のアドレスプールを選択する場合は、ネットマスクを 29 ビット以下にする必要があります。この理由は、OpenVPN はネットマスクが `/30`、`/31`、または `/32` のアドレスプールを扱えないからです。

Duplicate（重複）CN

ユーザが異なる IP アドレスから同時に接続できるようにする場合は、「*1ユーザ当たりの複数同時接続を許可*」を選択します。無効にすると、ユーザあたり 1つの同時 SSL VPN 接続のみが可能になります。

15.3.3 詳細

「*SSL > 詳細*」タブで、暗号化設定、圧縮設定、デバッグ設定など、各種の高度なサーバオプションを設定できます。

注 – このタブは「*サイト間 VPN > SSL*」および「*リモートアクセス > SSL*」で同じです。ここで加えた変更は、常に両方の SSL 設定に影響を与えます。

「暗号化設定」

これらの設定で、すべてのSSL VPNリモートアクセスクライアントの暗号化パラメータを制御します。

- **暗号化アルゴリズム:**暗号化アルゴリズムは、VPN トンネルを通して送信されるデータの暗号化に使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。

これらはすべて*暗号ブロック連鎖 (Cipher Block Chaining)*(CBC)モードで動作します。

- *DES-EDE3-CBC*
- *AES-128-CBC*(128ビット)
- *AES-192-CBC*(192ビット)
- *AES-256-CBC*(256ビット)
- *BF-CBC*(Blowfish(128ビット))

- **認証アルゴリズム:**認証アルゴリズムは、VPN トンネルを通して送信されるデータの完全性チェックに使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。
  - *MD5*(128ビット)
  - *SHA-1*(160ビット)
- **鍵サイズ:**鍵サイズ(鍵の長さ)とは、Diffie-Hellman 鍵交換の長さです。鍵が長ければ長いほど、対称鍵はセキュアになります。長さはビット単位で指定します。1024ビットまたは 2048 ビットの鍵サイズを選択できます。
- **サーバ証明書:**SSL VPN サーバがクライアントに対して自らの身元を証明するために使用するローカル SSL 証明書を選択します。
- **鍵ライフタイム:**鍵の有効期限を入力します。デフォルトは 28,800秒です。

圧縮設定

SSL VPN トラフィックの圧縮:有効にすると、SSL VPN トンネルを通して送信されるすべてのデータは、暗号化の前に圧縮されます。

デバッグ設定

デバッグモードの有効化:デバッグモードを有効にすると、デバッグに役立つ多くの情報が SSL VPN ログファイルに含まれます。

15.4 証明書管理

「*サイト間 VPN > 証明書管理*」「」メニューは、Sophos UTM の証明書関連のあらゆる操作を一元管理する場所です。たとえば、X.509 証明書の作成またはインポートや、CRL *(証明書失効リスト)*のアップロードなどを行うことができます。

15.4.1 証明書

*「サイト間 VPN > 証明書管理 > 証明書」*タブで、X.509 標準形式で公開鍵証明書を作成またはインポートできます。こうした証明書はデジタル署名された説明書で、通常は*認証局*(CA)が公開鍵および X.500 表記法による特定の*識別名*(DN)とともに発行します。

このタブで作成する証明書すべてには RSA 鍵が含まれています。これは、WebAdmin インタフェースへの初回ログイン時に提供した情報を使用して、自動的に作成された自己署名認証局「*VPN に署名する CA*」によって自己署名されます。

証明書を生成するには、以下の手順に従います。

1. **「*証明書*」タブで、「*新規証明書*」をクリックします。**
   「*証明書の追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:この証明書を説明する名前を入力してください。

   メソッド:証明書を作成するには、「*生成*」を選択します(証明書のアップロードに関する詳細は、以下を参照してください)。

   鍵サイズ:RSA 鍵の長さ。鍵は長ければ長いほど安全です。1024ビット、2048ビット、または4096ビットの鍵サイズを選択できます。使用する予定のアプリケーションやハードウェアデバイスと互換性のある最大鍵サイズを選択してください。長い鍵を使用することでパフォーマンスに深刻な問題が発生する場合を除き、パフォーマンスを最適化するために鍵の長さを削減しないようにしてください。

   VPN ID タイプ:証明書には一意の識別子を定義する必要があります。以下のタイプの識別子を使用できます。
   - メールアドレス
   - ホスト名
   - IP アドレス
   - 識別子(DN):

   VPN ID:選択した VPN ID タイプに応じて、このテキストボックスに適切な値を入力します。たとえば、「*VPN ID タイプ*」リストから「*IP アドレス*」を選択した場合、このテキストボックスに IP アドレスを入力します。このテキストボックスは、「*VPN ID タイプ*」リストで「*識別名*」を選択した場合は非表示になります。

ドロップダウンリストおよび「*国*」から「*メール*」までのテキストボックスを使用して、証明書の所持者を特定する情報を入力します。この情報は「*識別名*」を作成するために使用されます。つまり、その公開鍵を証明書が識別する団体の名前になります。この名前は X.500 標準の多数の個人情報を含み、インターネット上で一意であると想定されます。証明書がロードウォリア接続用である場合は、「*一般名*」ボックスにユーザ名を入力します。証明書がホスト用である場合は、ホスト名を入力します。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   証明書が「*証明書*」リストに表示されます。

証明書を削除するには、それぞれの証明書の「*削除*」ボタンをクリックします。

または、証明書をアップロードするには、以下の手順に従います。

1. **「*証明書*」タブで、「*新規証明書*」をクリックします。**
   「*証明書の追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:この証明書を説明する名前を入力してください。

   メソッド:「*アップロード*」を選択します。

   ファイルタイプ:証明書のファイルタイプを選択します。以下のいずれかのタイプの証明書をアップロードできます。

   - **PKCS#12(証明書+CA):**PKCS は、RSA ラボラトリにより考案され公開された「*公開鍵暗号標準*」(PKCS)のグループです。PKCS#12 ファイル形式は一般的に、秘密鍵を公開鍵証明書とともにコンテナのパスフレーズで保護して保存するために使用されます。この形式のファイルをアップロードするには、このコンテナパスフレーズを知っていることが必要です。
   - **PEM(証明書のみ):**パスワード不要の Base64 エンコードの「*プライバシー強化メール*」(PEM)ファイル形式。

   ファイル:「*ファイル*」ボックスの隣りのフォルダアイコンをクリックし、アップロードする証明書を選択します。

   コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   証明書が「*証明書*」リストに表示されます。

証明書を削除するには、それぞれの証明書の「*削除*」ボタンをクリックします。

証明書は PKCS#12 または PEM 形式でダウンロードできます。PEM ファイルは証明書だけを含みます。一方 PKCS#12 ファイルは、秘密鍵と署名に使用された CA 証明書を含んでいます。

15.4.2 認証局

*「サイト間 VPN > 証明書管理 > 認証局」*タブで、ユニットに新しい「*認証局*」を追加できます。一般的に、*認証局*(CA)は、他のパーティが使用するデジタル証明書を発行する機関です。CA は、証明書に含まれる公開鍵が、その証明書に記載された人、組織、ホスト、あるいは他のエンティティに属することを、CA 自身の証明書の秘密鍵を使って証明書の署名要求に署名することで証明します。このため、そのようなCAは署名 CA と呼ばれます。

UTM では、署名 CA は、UTM への初回のログイン時に提供した情報を使って自動的に作成されます。このように、「*証明書*」タブで作成するすべての証明書は、自己署名の証明書です。つまり、発行者と対象は同じになります。代わりに、サードパーティベンダの署名 CA をインポートすることもできます。さらに、IPsec 接続を要求するホストやユーザの真正性を確認する際に、秘密鍵が不明な別の CA 証明書を使用することもできます。これらの CA 証明書は検証 CA と呼ばれ、このタブで追加できます。

重要 – 使用しているシステムで複数の検証 CA を持つことができますが、署名 CA は 1つに限られています。新しい署名 CA をアップロードすると、以前インストールされた署名 CA は自動的に確認CAになります。

CA をインポートするには、以下の手順に従います。

1. **「*認証局*」タブで、「*CA をインポート*」をクリックします。**
   「*CA をインポート*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前:この CA を説明する名前を入力してください。

   タイプ:インポートする CA のタイプを選択します。確認 CA と署名 CA のいずれかを選択できます。確認 CA は PEM 形式で、署名 CA は PKCS#12 形式で利用できます。

   CA 証明書:「*CA 証明書*」ボックスの隣りのフォルダアイコンをクリックして、インポートする証明書を選択します。新しい署名 CA をアップロードする場合は、PKCS#12 コンテナに使用されていたパスワードを入力する必要があります。

   コメント(任意):説明などの情報を追加します。
3. **「*保存*」をクリックします。**
   新しい CA 証明書が「*認証局*」リストに表示されます。

CA を削除するには、それぞれの CA の「*削除*」ボタンをクリックします。

署名 CA は PKCS#12 形式でダウンロードできます。次にパスワードの入力を促すプロンプトが表示されます。このパスワードを使用して PKCS#12 コンテナのセキュリティが保護されます。また、検証 CA は PEM 形式でダウンロードできます。

15.4.3 証明書失効リスト(CRL)

CRL は、失効したために使用できない証明書（正確にはシリアル番号）のリストです。「*サイト間 VPN > 証明書管理 > 証明書失効リスト (CRL)*」タブで、PKI で使用している CRL をアップロードできます。

CRLをアップロードするには、以下の手順に従います。

1. **「*証明書失効リスト (CRL)*」タブで、「*CRL をアップロード*」をクリックします。**
   「*CRL をアップロード*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前:この CRL を説明する名前を入力してください。

   CRL ファイル:「*CRL ファイル*」ボックスの隣りのフォルダアイコンをクリックし、アップロードする CRL を選択します。

   コメント（任意）:説明などの情報を追加します。
3. **「*保存*」をクリックします。**
   新しい CRL が失効リストの一覧に表示されます。

CRL を削除するには、それぞれの CRL の「*削除*」ボタンをクリックします。

15.4.4 詳細

「*サイト間 VPN > 証明書管理 > 詳細*」タブで、ユニットの初期セットアップ時に作成された VPN 署名 CA を再生成できます。VPN 署名 CA は、リモートアクセスやサイト間 VPN 接続に使用されるデジタル証明書に署名する認証局です。古い VPN 署名 CA は、検証 CA として保持されます。

署名 CA の再生成

現在の署名 CA を使用してすべてのユーザ証明書を更新できます。この機能は「*認証局*」タブで別の VPN 署名 CA をインストールしたときに使用します。

警告 –UTM およびユーザ証明書は、新しい署名 CA を使って再生成されます。これによって、証明書を使用した、既存のサイト間 VPN 接続やリモートアクセス VPN 接続は使用できなくなります。

16 リモートアクセス

この章では、Sophos UTMのリモートアクセス設定の構成方法について説明します。Sophos UTMを使用したリモートアクセスは、*バーチャルプライベートネットワーク*(VPN)によって実現します。VPNは、在宅勤務の従業員などのリモートユーザに企業ネットワークへのアクセスを提供するためのセキュアでコスト効果の高い方法です。VPN は IPsec や PPTP などの暗号化トンネリングプロトコルを使用して、VPN で伝送されるデータの機密性とプライバシーを保護します。

参照 – リモートアクセス VPN 接続の設定方法の詳細は、Sophos サポートデータベースを参照してください。

UTMは、それぞれのリモートアクセス接続タイプに必要なインストールおよび設定ファイルを自動的に生成します。これらのファイルはユーザポータルから直接ダウンロードできます。ただし、ユーザには、使用可能な接続タイプに対応するファイルのみが提供されます。たとえば、SSL リモートアクセスを使用できるユーザには、SSL インストールファイルのみが提供されます。

注 – すべてのユーザまたは選択したユーザのリモートアクセス設定ファイルは、「*定義とユーザ*>*ユーザとグループ*>ユーザ」タブでダウンロードできます。

「*リモートアクセスステータス*」ページには、全オンラインユーザの概要が含まれます。

この章では、次のトピックについて説明します。

- SSL
- PPTP
- L2TP over IPsec
- IPsec
- HTML5 VPN ポータル
- Cisco VPN クライアント
- 詳細
- 証明書管理

16.1 SSL

Sophos UTM のリモートアクセス SSL 機能は、フル機能の SSL VPN ソリューションである OpenVPN によって実現します。これにより、お客様の会社とリモート従業員の間でポイントツーポイントの暗号化トンネルを作成することが可能になります。この機能では、インターネットリソースへのアクセスを許可するために、SSL証明書およびユーザ名/パスワードの組み合わせを必要とします。さらに、許可された各ユーザは、セキュアなユーザポータルから、カスタマイズされたSSL VPN クライアントソフトウェアバンドルをダウンロードできます。このバンドルには、無料のSSL VPN クライアント、SSL 証明書、およびワンクリックで簡単にインストールできる設定が含まれています。この SSL VPN クライアントは、ネイティブ Outlook、ネイティブ Windows ファイル共有などのほとんどのビジネスアプリケーションをサポートしています。

参照 – SSL VPN クライアントの使用方法に関する詳細は、Sophos サポートデータベースを参照してください。

16.1.1 プロファイル

「*リモートアクセス > SSL > プロファイル*」タブで、リモートアクセスユーザに対して異なるプロファイルを作成し、SSL VPN アクセスの基本設定を定義できます。

SSL VPN プロファイルを設定するには、以下の手順に従います。

1. **「*プロファイル*」タブで、「*新規リモート アクセス プロファイル*」をクリックします。**
   「*リモート アクセス プロファイルの追加*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   プロファイル名:このプロファイルを説明する名前を入力してください。

   ユーザとグループ:このプロファイルで SSL VPN リモートアクセスを使用できるようにするユーザとユーザグループを選択します。

   ローカルネットワーク:VPN SSL トンネル経由で選択した SSL クライアントへアクセス可能にするローカルネットワークを選択します。

   注 – デフォルトで、Sophos UTMの SSLVPN ソリューションは、いわゆるスプリットトンネリングを採用しています。これは、リモート VPN ユーザに VPN 上のリソースへのアクセスを許可すると同時に、インターネットなどのパブリックネットワークへのアクセスを許可するプロ

セスです。ただし、「*ローカルネットワーク*」フィールドで「*すべて*」を選択すると、スプリットトンネリングをバイパスできます。その結果、すべてのトラフィックが VPN SSL トンネル経由でルーティングされます。この場合、ユーザにパブリックネットワークへのアクセスを許可するかどうかは、ファイアウォールの設定によって決まります。

自動ファイアウォールルール:このオプションを選択すると、このプロファイル用のトラフィックを許可するファイアウォールルールを自動的に追加することができます。ルールは、プロファイルが有効になるとすぐに追加され、プロファイルが無効になると削除されます。このオプションを選択しない場合は、適切なファイアウォールルールを手動で指定する必要があります。

コメント(任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しいプロファイルが「*プロファイル*」リストに表示されます。

プロファイルを編集または削除するには、対応するボタンをクリックします。

注 – ユーザポータルの「*リモートアクセス*」メニューは、「*ユーザとグループ*」ボックスで選択されたユーザ、およびUTMにユーザ定義があるユーザのみが使用できます(「*定義とユーザ > ユーザとグループ > ユーザ*」を参照)。ユーザポータルへのログインに成功した認証されたユーザには、SSL VPN クライアントソフトウェアバンドルやインストール手順(Sophosサポートデータベース」で入手可能)へのリンクが提供されます。CA 証明書がインストールされていない場合や、ホスト名がポータル証明書にある一般名と一致しない場合、Android 環境の一部のブラウザでダウンロードに失敗する場合があります。この場合、ユーザは、CA 証明書をインストールするか、別のブラウザを使用する必要があります。

ライブログを開く

「*VPN ライブログを開く*」は、リモートアクセスアクティビティをログします。ボタンをクリックして、新しいウィンドウでライブログを開きます。

16.1.2 設定

「*SSL > 設定*」タブで、SSL VPN サーバ接続の基本設定を設定できます。

注 – このタブは「*サイト間 VPN > SSL*」および「*リモートアクセス > SSL*」で同じです。ここで加えた変更は、常に両方の SSL 設定に影響を与えます。

サーバ設定

SSLVPN 接続について以下の設定を行うことができます。

- **インタフェースアドレス:**デフォルトは「すべて」です。Web アプリケーションファイアウォールを使用する場合、サービスが SSL 接続をリスンするためのインタフェースアドレスを指定する必要があります。サイト間/リモートアクセス SSL 接続ハンドラと Web アプリケーションファイアウォールが受信 SSL 接続を識別できるようにするために、この設定が必要です。
- **プロトコル:**使用するプロトコルを選択します。*TCP* または *UDP* を選択できます。
- **ポート:**ポートを変更できます。デフォルトは `443` です。ポート `10443`、SUM ゲートウェイマネージャポート `4422`、または WebAdmin インタフェースが使用しているポートは使用できません。
- **ホスト名を上書き:**「*ホスト名を上書き*」ボックスの値は、クライアント VPN 接続のターゲットホスト名として使用され、デフォルトではゲートウェイのホスト名になります。システムの通常のホスト名（または DynDNS ホスト名）にこの名前でインターネットから到達できない場合のみ、デフォルトを変更します。

仮想 IP プール

プールネットワーク:これは、特定の IP 範囲から SSL クライアントに IP アドレスを配布するために使用される仮想 IP アドレスプールです。デフォルトでは、「*VPN プール (SSL)*」が選択されています。別のアドレスプールを選択する場合は、ネットマスクを 29 ビット以下にする必要があります。この理由は、OpenVPN はネットマスクが `/30`、`/31`、または `/32` のアドレスプールを扱えないからです。

Duplicate（重複） CN

ユーザが異なる IP アドレスから同時に接続できるようにする場合は、「*1ユーザ当たりの複数同時接続を許可*」を選択します。無効にすると、ユーザあたり 1つの同時 SSL VPN 接続のみが可能になります。

16.1.3 詳細

「*SSL > 詳細*」タブで、暗号化設定、圧縮設定、デバッグ設定など、各種の高度なサーバオプションを設定できます。

注 – このタブは「*サイト間 VPN > SSL*」および「*リモートアクセス > SSL*」で同じです。ここで加えた変更は、常に両方の SSL 設定に影響を与えます。

「暗号化設定」

これらの設定で、すべてのSSL VPNリモートアクセスクライアントの暗号化パラメータを制御します。

- **暗号化アルゴリズム:**暗号化アルゴリズムは、VPNトンネルを通して送信されるデータの暗号化に使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。これらはすべて*暗号ブロック連鎖 (Cipher Block Chaining)*(CBC)モードで動作します。
  - *DES-EDE3-CBC*
  - *AES-128-CBC*(128ビット)
  - *AES-192-CBC*(192ビット)
  - *AES-256-CBC*(256ビット)
  - *BF-CBC*(Blowfish(128ビット))
- **認証アルゴリズム:**認証アルゴリズムは、VPNトンネルを通して送信されるデータの完全性チェックに使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。
  - *MD5*(128ビット)
  - *SHA-1*(160ビット)
- **鍵サイズ:**鍵サイズ(鍵の長さ)とは、Diffie-Hellman鍵交換の長さです。鍵が長ければ長いほど、対称鍵はセキュアになります。長さはビット単位で指定します。1024ビットまたは2048ビットの鍵サイズを選択できます。
- **サーバ証明書:**SSL VPNサーバがクライアントに対して自らの身元を証明するために使用するローカルSSL証明書を選択します。
- **鍵ライフタイム:**鍵の有効期限を入力します。デフォルトは28,800秒です。

圧縮設定

SSL VPNトラフィックの圧縮:有効にすると、SSL VPNトンネルを通して送信されるすべてのデータは、暗号化の前に圧縮されます。

デバッグ設定

デバッグモードの有効化:デバッグモードを有効にすると、デバッグに役立つ多くの情報がSSL VPNログファイルに含まれます。

16.2 PPTP

PPTP (*Point-to-Point Tunneling Protocol*) により、単一のインターネットベースのホストは、暗号化トンネルを通して内部ネットワークサービスにアクセスすることが可能になります。PPTP の設定は容易で、Microsoft Windows システムでは特別なクライアントソフトウェアは必要ありません。

PPTP は Windows 95 以降の Microsoft Windows バージョンに含まれています。PPTP をSophos UTM で使用するには、クライアントコンピュータがMSCHAPv2 認証プロトコルをサポートすることが必要です。Windows 95 および 98 のユーザがこのプロトコルをサポートするには、システムに更新パッケージを適用する必要があります。

16.2.1 グローバル

グローバル PPTP オプションを設定するには、以下の手順に従います。

1. **「*グローバル*」タブで、PPTP リモートアクセスを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*メイン設定*」エリアが編集可能になります。

2. **次の設定を行います。**
   認証要求先:認証メカニズムを選択します。PPTP リモートアクセスは、ローカル認証と RADIUS 認証のみをサポートします。

   - **ローカル:**「*ローカル*」を選択する場合、PPTP リモートアクセスを使用できるようにするユーザとユーザグループを指定してください。バックエンドのユーザグループをフィールドにドラッグすることはできません。ユーザアカウントを指定するまでは、PPTP リモートアクセスはアクティブにできません。

     注 – 選択したユーザのユーザ名とパスワードには印刷可能な ASCII 文字しか使用できないことがあります[1]。

     注 – SSL VPN同様、ユーザポータルの「*リモートアクセス*」メニューにアクセスできるのは、「*ユーザとグループ*」ボックスで選択されたユーザと、ユーザ定義がUTMに定

[1] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters

義されているユーザのみです。ユーザポータルへのログインに成功した許可ユーザには、インストール手順（Sophos サポートデータベースで入手可能）へのリンクが提供されます。

- **RADIUS:***RADIUS* は、RADIUS サーバを事前に設定している場合にのみ選択できます。この認証方法では、ユーザは外部 RADIUS サーバに対して認証されます。このサーバは「*定義とユーザ > 認証サーバ > サーバ*」タブで設定できます。「*ユーザとグループ*」ダイアログボックスがグレーアウト表示されます。この設定はまだ変更できますが、影響はありません。RADIUS サーバは MSCHAPv2 チャレンジ/応答認証をサポートする必要があります。サーバはクライアントの IP アドレスや DNS/WINS サーバアドレスなどのパラメータを戻すことができます。PPTP モジュールは、NAS-ID として「`pptp`」を RADIUS サーバに送信します。RADIUS 認証を選択した場合は、ローカルユーザは PPTP では認証できなくなることに注意してください。さらに、クライアントは MSCHAPv2 認証もサポートする必要があることにも注意してください。

IP アドレスの割当て:IP アドレスは、事前に定義した IP アドレスプールから割り当てることも、DHCP サーバを使用して自動的に配布することもできます。

- **IP アドレスプール:**PPTP によってリモートアクセスするクライアントに特定の IP 範囲から IP アドレスを割り当てる場合は、このオプションを選択します。デフォルトでは、プライベート IP スペース `10.242.1.0/24` のアドレスが割り当てられます。このネットワーク定義は *VPN プール (PPTP)* と呼ばれ、すべてのネットワーク固有の設定オプションで使用できます。異なるネットワークを使用する場合は、*VPNプール (PPTP)* の定義を「*定義とユーザ > ネットワーク定義*」ページで変更します。または、「*プール ネットワーク*」テキストボックスの隣りの「＋」アイコンをクリックして、別の IP アドレスプールを作成することもできます。

- **DHCPサーバ:**「*DHCP サーバ*」を選択する場合、DHCP サーバが接続に使用するネットワークインタフェースも指定してください。DHCPサーバはインタフェースに直接接続する必要はありません。ルータを介してもアクセスできます。ローカル DHCP サーバはサポートされません。ここで選択した DHCP サーバは、物理的に異なるシステム上で稼働している必要があります。

3. **「*適用*」をクリックします。**
   設定が保存されます。

ライブログ

*PPTP デーモンライブログ*は、すべての PPTP リモートアクセスアクティビティをログします。ボタンをクリックして、新しいウィンドウでライブログを開きます。

16.2.2 iOS デバイス

ユーザポータルで iOS デバイスユーザに対し PPTP の自動設定を提供することができます。

ただし、「*グローバル*」タブの「*ユーザとグループ*」ボックスに追加されたユーザのみに対して、ユーザポータルサイトに設定ファイルが表示されます。iOS デバイスのステータスはデフォルトで有効になっています。

コネクション名:PPTP 接続を説明する名前を入力し、iOS デバイスのユーザがどの接続を確立しようとしているのか識別できるようにします。デフォルトの名前は、お客様の会社名の後に PPTP プロトコルが続いたものになります。

注 – 「*コネクション名*」はすべての iOS デバイス設定 (PPTP、L2TP over IPsec、Cisco VPN Client) で一意である必要があります。

ホスト名を上書き:システムのホスト名をクライアントがパブリックに解決できない場合は、ここにサーバのホスト名を入力して、これによって「*システムの DNS ホスト名*」の前の「*DynDNS ホスト名*」の内部設定を上書きします。

iOS デバイスの自動設定を無効にするには、トグルスイッチをクリックします。

トグルスイッチがグレーに変わります。

16.2.3 詳細

「*リモートアクセス > PPTP > 詳細*」タブで、暗号化の強度と PPTP リモートアクセスに関するデバッグ出力量を設定できます。PPTP の詳細オプションは、PPTP リモートアクセスのステータスが「*グローバル*」タブで有効になっていないと設定できません。

暗号強度

強い (128ビット) または弱い (40ビット) トンネル暗号化を選択できます (MPPE)。128ビット暗号化をサポートしないエンドポイントがない限り、弱い暗号化は使用しないでください。

デバッグモード

デバッグモードの有効化:このオプションで、PPTP ログで生成されるデバッグ出力の量を制御します。接続で問題が発生し、クライアントパラメータのネゴシエーションに関する詳細な情報が必要である場合などに、このオプションを選択します。

16.3 L2TP over IPsec

L2TP (*Layer Two (2) Tunneling Protocol*の略称) とは、既存のネットワーク (通常はインターネット) を介して 2つのピア間でネットワークトラフィックをトンネリングするためのデータリンクレイヤ (OSI モードのレイヤ2) プロトコルであり、VPN とも呼びます。L2TP プロトコルには機密性が欠けるため、多くの場合は機密性、認証、完全性を提供する IPsec と組み合わせて使用します。これら 2つのプロトコルの組み合わせを別名「L2TP over IPsec」と呼びます。L2TP over IPsec を使用すると、PPTP と同じ機能を提供しながら、暗号化された IPsec トンネル経由のネットワークアクセスを個々のホストに提供することができます。

16.3.1 グローバル

「*L2TP over IPsec* > *グローバル*」タブでは、L2TPover IPsec 経由のリモートアクセスをセットアップするための基本オプションを設定できます。

L2TP over IPsec を使用するには、次の手順に従ってください。

1. **「グローバル」タブで、L2TP over IPsec を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*サーバ設定および IP アドレス割り当て*」エリアが編集可能になります。

2. **次の設定を行います。**
   インタフェース:L2TP VPN アクセスに使用するネットワークインタフェースを選択します。

   認証モード:以下の認証モードから選択できます。

   - **事前共有鍵:**事前共有鍵として使用されるパスワードを入力します。*事前共有鍵*方式では、通信を行う前に、通信当事者間で共有シークレットを交換します。通信のためには、シークレットを知っていることを両者が証明します。共有シークレットとは、L2TP 用の暗号化アルゴリズムを使用してトラフィックを暗号化するために使用される安全なフレーズまたはパスワードです。セキュリティを高めるために、共有シークレットを強化する適切な手法をとる必要があります。共有シークレットのセキュリティは、パスワードの品質と、それをどれだけ安全に伝送するかにかかっています。一般的な言葉から成るパスワードは、辞書攻撃に対して非常に脆弱です。そのため、共有シークレットは非常に長くし、さまざまな文字、大文字、数字を組み合わせる必要があります。そのため、事前共有シークレットを使用する認証方式は、可能な限り

証明書方式に切り替える必要があります。

注 – iOS デバイスでは PSK 認証のみがサポートされているため、iOS デバイスへのアクセスを有効にするためには、*事前共有鍵*を選択する必要があります。

- **X.509 CA チェック:**X.509 証明書により、参加者の多い大規模な VPN セットアップでの公開認証鍵の交換が容易になります。いわゆる CA が VPN エンドポイントの公開鍵を収集してチェックし、各メンバに対して証明書を発行します。証明書には、ピアのアイデンティティと公開鍵が含まれています。証明書はデジタル署名されているため、検出されずに他人が偽造証明書を発行することはできません。
  鍵交換中に証明書が交換され、ローカル保存された CA 公開鍵を使用して検証されます。続いて、公開鍵とプライベート鍵を使用して VPN エンドポイントの実際の認証が行われます。この認証モードを使用するためには、X.509 証明書を選択します。
  X.509 認証が機能するためには、「*リモートアクセス > 証明書管理 > 認証局 (CA)*タブで有効な CA を設定する必要があります。

IP アドレスの割当て:IP アドレスは、事前に定義した IP アドレスプールから割り当てることも、DHCP サーバを使用して自動的に配布することもできます。

- **プールネットワーク:**デフォルトでは、IP アドレスの割当方法として「*IP アドレスプール*」が選択されており、「*プールネットワーク*」には事前定義済みの「*VPN プール (L2TP)*」ネットワーク定義が選択されています。*VPN プール (L2TP)*とは、プライベートインターネット用の IP アドレススペース `10.x.x.x` からクラス C サブネットを使用してランダムに生成されたネットワークです。これは、ユーザが接続元として専用のアドレスプールを持つことを保証するものであり、通常は一切変更する必要がありません。別のネットワークを使用したい場合は、「*VPN プール (L2TP)*」の定義を変更するか、ここで IP アドレスプールとして他のネットワークを割り当てます。

注 – L2TP VPN プールに対してプライベート IP アドレスを使用しており、インターネットへのアクセスに IPsec ホストを許可したい場合、適切なマスカレーディングまたは NAT ルールを IP アドレスプールに用意する必要があります。

- **DHCPサーバ:**「*DHCP サーバ*」を選択する場合、DHCP サーバが接続に使用するネットワークインタフェースも指定してください。DHCPサーバはインタフェースに直接接続する必要はありません。ルータを介してもアクセスできます。ローカル DHCP サーバはサポートされません。ここで選択した DHCP サーバは、物理的に異なるシステム上で稼働している必要があります。

3. **「*適用*」をクリックします。**
   設定が保存されます。

   設定をキャンセルするには、アンバー色のトグルスイッチをクリックします。

アクセス制御

認証要求先:L2TP リモートアクセスは、ローカル認証とRADIUS 認証のみをサポートします。

- **ローカル:**「*ローカル*」を選択する場合、L2TP リモートアクセスを使用できるようにするユーザとユーザグループを指定してください。バックエンドのユーザグループをフィールドにドラッグすることはできません。ローカルユーザの場合、通常の方法でユーザを追加し、これらのユーザに対して L2TP を有効にします。ユーザまたはグループを選択しない場合、L2TP リモートアクセスはオフになります。

  注 – 選択したユーザのユーザ名とパスワードには印刷可能な ASCII 文字しか使用できないことがあります([1])。

  注 –SSLVPN同様、ユーザポータルの「*リモートアクセス*」メニューにアクセスできるのは、「*ユーザとグループ*」ボックスで選択されたユーザと、ユーザ定義がUTMに定義されているユーザのみです。認証モードに応じて、ユーザポータルへのログインに成功した認証ユーザには、IPsec 事前共有鍵(認証モード「*事前共有鍵*」)または `PKCS#12` ファイル(認証モード「*X.509 CA チェック*」)ならびにインストール手順(Sophos サポートデータベースで入手可能)へのリンクが提供されます。

- **RADIUS:**「*RADIUS*」を選択すると、認証要求は RADIUS サーバに転送されます。L2TP モジュールは、NAS-IDとして「`l2tp`」を RADIUS サーバに送信します。

クライアントとサーバ間で、認証アルゴリズムのネゴシエーションが自動的に行われます。ローカルユーザに対し、Sophos UTMは次の認証プロトコルをサポートしています。

- MSCHAPv2
- PAP

デフォルトで、Windows クライアントは MSCHAPv2 をネゴシエーションします。

RADIUSユーザに対し、Sophos UTMは次の認証プロトコルをサポートしています。

[1] http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters

- MSCHAPv2
- MSCHAP
- CHAP
- PAP

16.3.2 iOS デバイス

ユーザポータルで iOS デバイスユーザに対し自動 L2TP over IPsec 設定を提供することができます。

ただし、「*グローバル*」タブの「*ユーザとグループ*」ボックスに追加されたユーザのみに対して、ユーザポータルサイトに設定ファイルが表示されます。iOS デバイスのステータスはデフォルトで有効になっています。

コネクション名:L2TP over IPsec 接続を説明する名前を入力し、iOS デバイスのユーザがどの接続を確立しようとしているのか識別できるようにします。デフォルトの名前は、お客様の会社名の後に L2TP over IPsec プロトコルが続いたものになります。

注 – 「*コネクション名*」はすべての iOS デバイス設定 (PPTP、L2TP over IPsec、Cisco VPN Client) で一意である必要があります。

ホスト名を上書き:システムのホスト名をクライアントがパブリックに解決できない場合は、ここにサーバのホスト名を入力して、これによって「*システムの DNS ホスト名*」の前の「*DynDNS ホスト名*」の内部設定を上書きします。

iOS デバイスの自動設定を無効にするには、トグルスイッチをクリックします。

トグルスイッチがグレーに変わります。

16.3.3 デバッグ

IKEデバッグ

「*IKE デバッグ*」セクションで IKE デバッグオプションを設定できます。どのタイプの IKE メッセージまたは通信についてデバッグ出力を作成するかはチェックボックスで選択します。

注 – 「*IKE デバッグ*」セクションは、「*サイト間 VPN IPsec*」、「*リモートアクセス IPsec*」、「*L2TP over IPsec*」、および「*Cisco VPN クライアント*」メニューの「デバッグ」タブで同じものが使用されています。

以下のフラグをログできます。

- **コントロールフロー:**IKE ステートのコントロールメッセージを表示します。
- **アウトバウンドパケット:**送信 IKE メッセージのコンテンツを表示します。
- **インバウンドパケット:**受信 IKE メッセージのコンテンツを表示します。
- **カーネルメッセージ:**カーネルとの通信メッセージを表示します。
- **冗長構成 (HA)**その他の HA ノードとの通信を表示します。

L2TP デバッグ

「*デバッグモードを有効にする*」を選択すると、*IPsec VPN* ログファイルに、L2TP または PPP 接続ネゴシエーションに関する多くの情報が含まれるようになります。

16.4 IPsec

IPsec (IP Security) とは、すべての IP パケットを暗号化または認証すること (あるいはその両方) によって IP *(インターネットプロトコル)* 通信のセキュリティを維持するための標準です。

IPsec 標準は、次の 2つのサービスモードと2つのプロトコルを定義しています。

- トランスポートモード
- トンネルモード
- *AH (認証ヘッダ)* 認証プロトコル
- *ESP (カプセル化セキュリティペイロード)* 暗号化 (および認証) プロトコル

IPsec には、SA *(セキュリティアソシエーション)* と鍵配布を手動および自動で管理するための方法も用意されています。これらの特徴は、DOI *(解釈ドメイン)* で一元管理されています。

IPsec モード

IPsec は、トランスポートモードまたはトンネルモードで機能します。原則的に、ホスト間接続ではどちらのモードも使用できます。ただし、いずれかのエンドポイントがセキュリティゲートウェイである

場合、トンネルモードを使用する必要があります。この UTM での IPsec VPN 接続では、常にトンネルモードが使用されます。

トランスポートモードでは、元の IP パケットは他のパケットにカプセル化されません。元の IP ヘッダは維持され、パケットの残りの部分は平文のまま(AH)またはカプセル化されて(ESP)送信されます。パケット全体を AH で認証することも、ESP でペイロードをカプセル化して認証することもできます。いずれの場合も、元のヘッダは平文として WAN 経由で送信されます。

トンネルモードでは、パケットヘッダとペイロードの全体が新しい IP パケットにカプセル化されます。IP ヘッダが IP パケットに追加され、宛先アドレスは受信側トンネルエンドポイントに設定されます。カプセル化パケットの IP アドレスは変更なしで維持されます。続いて、元のパケットが AH で認証されるか、ESP でカプセル化されて認証されます。

IPsec プロトコル

IPsec では、IP レベルで安全に通信するために 2つのプロトコルを使用します。

- **AH (認証ヘッダ):**パケット送信者を認証し、パケットデータの完全性を保証するためのプロトコル。
- **カプセル化セキュリティペイロード (ESP):**パケット全体を暗号化し、そのコンテンツを認証するためのプロトコル。

AH *(認証ヘッダ)*プロトコルは、パケットデータの信頼性と完全性をチェックします。さらに、送信者と受信者の IP アドレスが送信中に変更されていないことをチェックします。パケットは、ハッシュベースの*メッセージ認証コード*(HMAC)と鍵を使用して作成されたチェックサムを使用して認証されます。次のいずれかのハッシュアルゴリズムが使用されます。

- **MD5 (メッセージダイジェスト、バージョン 5):**このアルゴリズムでは、任意のサイズのメッセージから 128ビットのチェックサムが生成されます。このチェックサムはメッセージの指紋のようなもので、メッセージが変更されるとチェックサムも変わります。このハッシュ値は、デジタル署名またはメッセージダイジェストとも呼ばれます。
- **SHA-1 (セキュアハッシュ):**このアルゴリズムでは MD5 と類似したハッシュが生成されますが、SHA-1 ハッシュは長さが 160ビットです。SHA-1 は鍵が MD5 より長いため、MD5 より強力なセキュリティが実現します。

MD5 と比較すると、SHA-1 ハッシュは計算が難しく、生成に必要な CPU 時間はより長くなります。もちろん、計算速度は、プロセッサの処理速度とSophos UTMで使用される IPsec VPN 接続の数に依存します。

ESP *(カプセル化セキュリティペイロード)*プロトコルには、暗号化以外に、送信者を認証し、パケットコンテンツを検証する機能もあります。トンネルモードで ESP を使用すると、IP パケット全体 (ヘッダ

とペイロード）が暗号化されます。ここで、暗号化されていない IP ヘッダと ESP ヘッダがカプセル化するパケットに追加されます。新しい IP ヘッダには、受信側ゲートウェイと送信側ゲートウェイのアドレスが含まれています。これらの IP アドレスは、VPN トンネルのアドレスです。

暗号化付きの ESP では、通常次のアルゴリズムが使用されます。

- 3DES（トリプルデータ暗号化標準）
- AES（高度暗号化標準）

これらのうち、AES が最も安全です。AES で使用可能な鍵の有効長は 128ビット、192ビット、256ビットです。Sophos UTMSophos UTM は、多数の暗号化アルゴリズムをサポートしています。認証には MD5 または SHA-1 アルゴリズムを使用できます。

NATトラバーサル（NAT-T）

NAT トラバーサルとは、NAT デバイスを使用する TCP/IP ネットワーク内のホスト間で接続を確立するための技術です。この接続は、ESP パケットの UDP カプセル化を使用して、NAT デバイス経由で IPsec トンネルを確立することによって実現します。UDP カプセル化は、IPsec ピア間で NAT が検出された場合のみに使用されます。検出されなかった場合は、通常の ESP パケットが使用されます。

NAT トラバーサルにより、ゲートウェイまたはロードウォリアを NAT ルータの背後に配置しながら、IPsec トンネルを確立できるようになります。この機能を使用する場合、両方の IPsec ピアで NAT トラバーサルがサポートされている必要があります。ネゴシエーションは自動的に行われます。NAT デバイスで IPsec パススルーがオフになっていることを確認してください。オンになっていると、NAT トラバーサルの使用に支障が出る可能性があります。

ロードウォリアで NAT トラバーサルを使用する場合、WebAdmin 内の対応ユーザオブジェクトに静的なリモートアクセス IP アドレス（RAS アドレス）が設定されている必要があります（WebAdmin の「ユーザ」ページの「*リモートアクセスにスタティック IP アドレスを使用*」も参照してください）。

データ未送信時に確立されたトンネルが期限切れになることを防ぐために、NAT トラバーサルの keep-alive 信号がデフォルトで 60秒間隔で送信されます。keep-alive メッセージは、NAT ルータがセッションに関連するステート情報を維持しており、トンネルが開いたままであることを確認するために送信されます。

TOS

「サービスタイプ」ビット（TOS ビット）は、IP ヘッダにあるいくつかの 4ビットフラグです。これらのビットは、どのタイプのサービス品質が必要であるかを転送アプリケーションがネットワークに伝えるこ

とを許可するため、*サービスタイプ*ビットと呼ばれています。

Sophos UTMへの IPsec 導入では、TOS の値は常にコピーされます。

16.4.1 コネクション

「*IPsec > コネクション*」タブでは、IPsec コネクションを作成し、編集することができます。

IPsec コネクションを作成するには、次の手順に従います。

1. **「コネクション」タブで「*新規 IPsec リモートアクセスルール*」をクリックします。**
   「*IPsec リモートアクセスルールの追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:この接続を説明する名前を入力してください。

   インタフェース:IPsec トンネルのローカルエンドポイントとして使用されるインタフェースの名前を選択します。

   ローカルネットワーク:VPN トンネル経由でアクセス可能にするローカルネットワークを選択します。

   仮想 IP プール:クライアントにスタティック IP アドレスが定義されていない場合、クライアントはこの IP アドレスプールに割り当てられた IP アドレスを取得します。デフォルトプールは *VPN プール (IPsec)* であり、プライベート IP スペース `10.242.4.0/24` から成ります。ただし、他の IP アドレスプールを選択または作成することもできます。

   ポリシー:この IPsec コネクションの IPsec ポリシーを選択します。IPsec ポリシーは、「*リモートアクセス > IPsec > ポリシー*」タブで定義できます。

   認証タイプ:このリモートゲートウェイ定義の認証タイプを選択します。次のタイプを使用できます。

   - **事前共有鍵:**「*事前共有鍵*」(PSK) による認証では、秘密のパスワードを鍵として使用します。これらのパスワードは、接続を確立する前にエンドポイントに配布する必要があります。新しい VPN トンネルが確立されると、両端で、相手側が秘密のパスワードを知っていることのチェックが行われます。PSK のセキュリティは、使用するパスワードの品質に依存します。一般的な言葉や成句では、辞書攻撃に対して脆弱です。常時の、または長期的な IPsec コネクションでは、パスワードの代わりに証明書を使用すべきです。

   - **X.509 証明書:**X.509 証明書による認証方式では、公開鍵と秘密鍵を使用します。X.509 証明書には、公開鍵と、鍵の所有者を特定する情報が含まれています。このような証明書は、信頼される*認証局* (CA) によって署名され、発行されたもので

す。選択後、この IPsec コネクションの使用を許可するユーザを指定します。バックエンドユーザグループを「*許可ユーザ*」フィールドにドラッグすることはできません。「*自動ファイアウォールルール*」チェックボックスにチェックを入れた場合を除き、適切なファイアウォールルールを「*ネットワークプロテクション*」メニューに手動で指定する必要があります。

注 – ユーザポータルにアクセスできるのは、「*許可されるユーザ*」ボックスで選択されており、UTMにユーザ定義が存在するユーザのみです。ユーザポータルへのログインに成功した認証されたユーザには、*Sophos IPsec Client* (SIC)、設定ファイル、PKCS#12ファイル、インストール手順 (Sophos サポートデータベースで入手可能) へのリンクが提供されます。

- **CA DN 照合**:この認証タイプでは、CA 証明書の DN *(識別名)* の照合を使用して、VPN エンドポイントの鍵を検証します。選択した場合、*認証局*を 1つ選択し、リモートアクセスクライアントの DN と一致する *DN マスク*を選択します。ここで、「*ピアサブネット範囲*」を選択または追加します。クライアントは、いずれかの証明書が DN マスクと一致しなければ接続が許可されません。

XAUTH の有効化 (オプション):設定されたバックエンドに対するユーザ認証が必要である場合は、拡張認証を有効にする必要があります。

自動ファイアウォールルール (オプション):このオプションは、認証タイプ *X.509 証明書*のみで使用可能です。このオプションを選択すると、この接続用のトラフィックを許可するファイアウォールルールを自動的に追加することができます。ルールは、接続が確立するとすぐに追加され、接続が無効になると削除されます。

コメント (任意):説明などの情報を追加します。

3. **「*保存*」をクリックします。**
   新しいリモートアクセスルールが「*コネクション*」リストに表示されます。

リモートアクセスルールを編集または削除するには、対応するボタンをクリックします。

16.4.2 ポリシー

「*リモートアクセス > IPsec > ポリシー*」タブでは、IPsec コネクションのパラメータをカスタマイズし、ポリシーに統合することができます。IPsec ポリシーは、IPsec コネクションの IKE (インターネット鍵交換) と IPsec プロポーザルパラメータを定義します。それぞれの IPsec コネクションには IPsec ポリシーが必要です。

注 – Sophos UTM は、IKE フェーズ 1 のメインモードのみをサポートしています。アグレッシブモードはサポートされていません。

IPsec ポリシーを作成するには、以下の手順に従います。

1. **「*ポリシー*」タブで、「*新規 IPsec ポリシー*」をクリックします。**
   「*IPsec ポリシーの追加*」ダイアログボックスが開きます。

2. **次の設定を行います。**
   名前:このポリシーを説明する名前を入力します。

   IKE 暗号化アルゴリズム:暗号化アルゴリズムでは、IKE メッセージの暗号化に使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。

   - *DES*(56ビット)
   - *3DES*(168ビット)
   - *AES 128*(128ビット)
   - *AES 192*(192ビット)
   - *AES 256*(256ビット)
   - *Blowfish*(128ビット)
   - *Twofish*(128ビット)
   - *Serpent*(128ビット)

   セキュリティに関する注記 – DES の使用は推奨されません。アルゴリズムの強度が低いため、脆弱性につながる可能性があります。

   IKE 認証アルゴリズム:認証アルゴリズムでは、IKE メッセージの完全性チェックに使用するアルゴリズムを指定します。以下のアルゴリズムがサポートされています。

   - *MD5*(128ビット)
   - *SHA1*(160ビット)
   - *SHA2 256*(256ビット)
   - *SHA2 384*(384ビット)
   - *SHA2 512*(512ビット)

IKE SA ライフタイム:この値には、IKE SA（セキュリティアソシエーション）が有効な期間（つまり次の鍵更新を行うタイミング）を秒単位で指定します。有効な値は 60秒～28800秒（8時間）です。デフォルト値は 7800秒です。

IKE DH グループ:接続をネゴシエートする際は、通信するパーティはデータの暗号化に使用する実際の鍵についても取り決めます。IKE はセッション鍵を生成するために、ランダムデータを利用する *Diffie–Hellman*（DH）アルゴリズムを使用します。ランダムデータの生成はプールビットに基づいて行われます。基本的には IKE グループがプールビット数を知らせます。プールビット数が多いほど、ランダムな数字が大きくなります。数字が大きいほど、Diffie–Hellman アルゴリズムの解読は難しくなります。結果として、プールビット数が多ければ安全ですが、CPU の使用量も増えます。現在は以下の Diffie–Hellman グループがサポートされています。

- *Group 1:MODP 768*
- Group 2:MODP 1024
- *Group 5:MODP 1536*
- *Group 14:MODP 2048*
- *Group 15:MODP 3072*
- *Group 16:MODP 4096*

セキュリティに関する注記 – グループ1（MODP 768）は弱く、相互運用性の理由のみからサポートされています。使用は推奨されません。脆弱性につながる可能性があります。

IPsec 暗号化アルゴリズム:IKE の場合と同じ暗号化アルゴリズム。さらに、以下のエントリもあります。

- *暗号化なし（null）*
- *AES 128 CTR*（128ビット）
- *AES 192 CTR*（192ビット）
- *AES 256 CTR*（256ビット）
- *AES 128 GCM（96ビット）*
- *AES 192 GCM（96ビット）*
- *AES 256 GCM（96ビット）*
- *AES 128 GCM（128ビット）*

- *AES 192 GCM (128ビット)*
- *AES 256 GCM (128ビット)*

セキュリティに関する注記 – 暗号化を実行しないこと、または DES の使用は推奨されません。脆弱性につながる可能性があります。

IPsec 認証アルゴリズム:IKE の場合と同じ認証アルゴリズム。さらに、以下のアルゴリズムもあります。

- *SHA2 256* (96ビット)
- *SHA2 384* (96ビット)
- *SHA2 512* (96ビット)

これらは、バージョン 8 より古い UTM (つまり ASG) など、RFC 4868 に準拠していないトンネルエンドポイント用です。切り捨てられたチェックサムで 96ビットより長いものには対応していません。

IPsec SA ライフタイム:この値には、IPsec SA が有効な期間 (つまり次の鍵更新を行うタイミング) を秒単位で指定します。有効な値は 60秒～86400秒 (1日) です。デフォルト値は 3600秒です。

IPsec PFS グループ: *Perfect Forward Secrecy* (PFS) という概念では、セッション鍵を使用できなくなった場合に、この特定セッションのデータにのみアクセスを許可します。PFS が存在するには、IPsec SA の保護に使用される鍵は、IKE SA の鍵を取得するために使用されるランダム鍵作成用のマテリアルから派生したものではないことが必要です。その場合、PFS は 2回目の Diffie-Hellman 鍵交換を開始し、IPsec 接続に対して選択された DH グループが新たにランダム生成された鍵を取得することを提案します。サポートされている Diffie-Hellman グループは IKE の場合と同じです。
PFS を有効にすると安全性が高まりますが、交換にさらに時間がかかるようになります。低速なハードウェアでは PFS は使用しないことをお勧めします。

注 – PFS はすべてのベンダーとの完全な相互運用性はありません。ネゴシエーション時に問題が発生したら、PFS を無効にしてください。

厳密ポリシー:IPsec ゲートウェイが暗号化アルゴリズムおよびその強度について提案を行うと、IPsec ポリシーがそれに対応していない場合でも、受信側ゲートウェイがこの提案を受け入れる場合があります。このオプションを選択すると、指定したパラメータを厳密にそのと

おり使用することについてリモートエンドポイントが合意しないときは、IPsec 接続は確立されません。UTMの IPsec ポリシーが AES-256 暗号化を必要とする際に、SSH Sentinel を使用するロードウォリアが AES-128 を使用して接続しようとすると、厳格なポリシーオプションが有効である場合は、接続は拒否されます。

注 – 圧縮の設定は「*ストリクトポリシー*」を介しては施行されません。

圧縮:*IP ペイロード圧縮プロトコル*(IPComp)によってIPパケットを暗号化の前に圧縮するかどうかを指定します。IPComp は IP パケットを圧縮してそのサイズを縮小し、通信ホストまたはゲートウェイのペア間の全体的な通信パフォーマンスを向上させます。デフォルトでは圧縮はオフになっています。

コメント(任意):説明などの情報を追加します。

3. **「保存」をクリックします。**
   新しいポリシーが「*ポリシー*」リストに表示されます。

ポリシーを編集または削除するには、対応するボタンをクリックします。

16.4.3 詳細

「*リモートアクセス > IPsec > 詳細*」タブで、IPsec VPN の詳細オプションを設定できます。希望の認証タイプに応じて、ローカル証明書 (X.509 認証の場合) やローカル RSA 鍵 (RSA 認証の場合) などを定義可能です。この設定は熟練ユーザのみが行ってください。

ローカル X.509 証明書

X.509 認証では、証明書を使用して VPN エンドポイントの公開鍵を検証します。この認証タイプを使用する場合は、「*ローカル X.509 証明書*」エリアのドロップダウンリストからローカル証明書を選択する必要があります。選択した鍵/証明書は、X.509 認証が選択された場合のリモートピアへのゲートウェイの認証に使用されます。

適切な秘密鍵がある証明書のみ選択できます。他の証明書はこのドロップダウンリストでは利用できません。

選択できる証明書がない場合、新しい証明書を作成するか、またはアップロード機能を使用してインポートして、「*証明書管理*」メニューで追加する必要があります。

証明書を選択したら、秘密鍵を保護するパスフレーズを入力します。パスフレーズは保存プロセスで確認され、パスフレーズが暗号化鍵と一致しない場合はエラーメッセージが表示されます。

アクティブな鍵/証明書を選択すると、それは「*ローカル X.509 証明書*」エリアに表示されます。

デッドピア検出 (DPD)

デッドピア検出 (DPD)を使用デッドピア検出オプションを使用して、リモート VPN ゲートウェイあるいはクライアントに接続できない場合は接続を自動的に終了します。スタティックエンドポイントとの接続では、トンネルは自動的に再ネゴシエートされます。ダイナミックエンドポイントとの接続では、リモート側でトンネルの再ネゴシエートを行うことが必要です。通常はこのオプションを常に有効にしておくほうが安全です。IPsecピアはリモート側がデッドピア検出をサポートするかどうかを自動的に判断し、必要に応じて通常モードにフォールバックします。

NAT トラバーサル (NAT-T)

NATトラバーサルを使用:このオプションを選択すると、IPsecトラフィックは、「*ネットワークアドレス変換*」(NAT)を使用するアップストリームシステムを通過できるようになります。さらに、NATトラバーサルのキープアライブ(keepalive)間隔を定義できます。 設定を保存するには「*適用*」をクリックします。

CRL処理

証明書のプロバイダが、まだ有効な証明書に与えられる承認を取り消す場合があるかもしれません。たとえば、証明書の受取人が不正なデータ(名前など)を使ってそれを不正に取得したことが判明した場合や、証明書に埋め込まれた公開鍵の一部である秘密鍵を攻撃者が入手した場合は、証明書が失効します。そのような場合に備えて、いわゆる*証明書失効リスト*(CRL)が使用されます。CRL には通常、依然として有効期間は残っているものの無効とされた証明書のシリアル番号が含まれています。
これらの有効期限が切れると、証明書は無効になり、ブロックリストから削除されます。

自動取得:この機能は、HTTP、Anonymous(匿名)FTP、または LDAP バージョン 3を介しパートナー証明書で定義された URL を通して CRL を要求します。有効期限が切れたら、要求によって CRL をダウンロードし、保存して更新できます。この機能を、ポート80 または 443を経由せずに使用する場合は、適切なファイアウォールルールを設定して、CRL 配布サーバにアクセスできるようにしてください。

厳密ポリシー:このオプションを有効にすると、対応する CRL のないパートナー証明書は拒否されます。

PSK プローブ:

応答のみモードを使用したIPsec接続では、それぞれの IPsec 接続に対して別々の事前共有鍵(PSK)を使用することを選択できます。

PSKプローブの有効化このチェックボックスにチェックを入れて、このオプションを有効にします。この設定は、L2TP-over-IPsec、リモートアクセス IPsec、VPN IPsec の各接続に影響を与えます。

16.4.4 デバッグ

IKE デバッグ

「*IKE デバッグ*」セクションで IKE デバッグオプションを設定できます。どのタイプの IKE メッセージまたは通信についてデバッグ出力を作成するかはチェックボックスで選択します。

注 – 「*IKE デバッグ*」セクションは、「*サイト間 VPN IPsec*」、「*リモートアクセス IPsec*」、「*L2TP over IPsec*」、および「*Cisco VPN クライアント*」メニューの「*デバッグ*」タブで同じものが使用されています。

以下のフラグをログできます。

- **コントロールフロー:**IKE ステートのコントロールメッセージを表示します。
- **アウトバウンドパケット:**送信 IKE メッセージのコンテンツを表示します。
- **インバウンドパケット:**受信 IKE メッセージのコンテンツを表示します。
- **カーネルメッセージ:**カーネルとの通信メッセージを表示します。
- **冗長構成 (HA)**その他の HA ノードとの通信を表示します。

16.5 HTML5 VPN ポータル

HTML5 VPNポータル機能を使用すると、外部ネットワークのユーザは、プラグインをインストールしなくても、ブラウザのみをクライアントとして使用して、あらかじめ設定されているコネクションタイプで内部リソースにアクセスすることができます。このためには、ユーザはUTMのユーザポータルにログインする必要があります。このポータルの**【***HTML5 VPNポータル(HTML5 VPN Portal)***】**タブには、このユーザが使用できる全コネクションのリストが表示されます。**【***接続(Connect)***】**ボタンをクリックすると、定義されている内部リソースへの接続が開始されます。管理者は、許可ユーザ、コネクションタイプ、その他の設定を指定して、事前にこれらのコネクションを作成する必要があります。内部リソースへのアクセスには、リモートデスクトップにアクセスするためのリモートデスクトッププロトコル(RDP)か仮想ネットワークコンピューティング(VNC)、Webアプリケーション(HTTP/HTTPS)を使用するためのブラウザ、ターミナルセッション用のTelnet/セキュアシェル(SSH)など、各種のコネクションタイプを使用できます。しかし、HTML 5 VPN ポータルでは、ユーザのローカルコンピュータに、コンテンツをダウンロードすることは許可されません(例:HTTP 経由など)。

この機能を使用すると、それ自体ではマルチユーザアクセスをサポートしない内部リソース(スイッチのようなネットワークハードウェアなど)への複数ユーザのアクセスを許可したり、システムまたはネットワーク全体へのアクセスを許可するのではなく、1つのサービスのみに絞った詳細なアクセス管理を簡単に行うことができます。

例:

- 電話システムを保守する電話サービス会社にアクセスを提供。
- イントラネットなど、特定の内部Webサイトへのアクセスを提供。

注 – ブラウザは HTML5 に準拠したものである必要があります。HTML5 VPN 機能に対応しているブラウザは次のとおりです。Firefox 6.0 以降、Internet Explorer 10 以降、Chrome、Safari 5 以降(Mac 環境のみ)。

16.5.1 グローバル

「*リモートアクセス > HTML5 VPN ポータル > グローバル*」タブでは、HTML5 VPN ポータルを有効化し、各 VPN ポータルコネクションを管理できます。許可されたユーザの場合、ユーザポータルの「*HTML5 VPN ポータル*」タブで有効な接続を使用できます。

HTML5 VPN ポータルを有効化して、新規 HTML5 VPN コネクションを作成するには、次の手順に従います。

1. **HTML5 VPN ポータルを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色になり、「*接続*」エリアが編集可能になります。許可されているユーザには、有効にされている既存の全コネクションがユーザポータルに表示されます。

2. **「*新規 HTML5 VPN ポータルコネクション*」ボタンをクリックします。**
   「*HTML5 VPN ポータルコネクションの追加*」ダイアログボックスが開きます。

3. **次の設定を行います。**
   名前:この接続を説明する名前を入力してください。

   コネクションタイプ:接続タイプを選択します。選択したコネクションタイプによっては、異なるパラメータが表示されます。次のタイプを使用できます。

   - **リモートデスクトップ:**Windows ホストでリモートデスクトップセッションを開始する場合など、リモートデスクトッププロトコル(RDP)を使用したリモートアクセス。

- **Webapp (HTTP):**HTTP を使用した Web アプリケーションへのブラウザベースのアクセス。
- **Webapp (HTTPS):**HTTPS を使用した Web アプリケーションへのブラウザベースのアクセス。

  注 – HTTP/HTTPS 接続に使用される URL は、このコネクションの「*宛先*」、「*ポート*」、および「*パス*」オプションから構成されます。Web アプリケーションは Mozilla Firefox (バージョン 6.0 以降) に対応している必要があります。

- **Telnet:**スイッチやプリンタにアクセスを提供する場合などの、Telnet プロトコルを使用したターミナルアクセス。
- **SSH:**SSH を使用したターミナルアクセス。
- **VNC:**Linux/Unix ホストのリモートデスクトップを開く場合などの、仮想ネットワークコンピューティング (VNC) を使用したリモートアクセス。

  注 – 現在は VNC の従来の認証 (パスワードのみ) のみがサポートされています。サーバがが正しく設定されていることを確認してください。

宛先:許可されたユーザが接続できるホストを追加します。

注 – 選択した宛先ホストが自己署名証明書を提供する場合、証明書の CN (一般名) が宛先ホスト名と一致することを確認してください。一致しない場合は、ポータルのブラウザに証明書警告が出ます。たとえば、DNS ホストとして *www.mydomain.com* を使用する場合、自己署名証明書にこの名前が含まれることを確認してください。DNS ホストの代わりにホストを使用する場合、ホストの IP アドレスが *SAN (Subject Alternative Name)* として自己署名証明書に含まれていることを確認してください。

パス (コネクションタイプが *Webapp* のみ):許可されたユーザが接続できるパスを入力します。

ユーザ名 (コネクションタイプが *SSH* のみ):ユーザが接続に使用するユーザ名を入力します。

自動ログイン/自動ログイン (基本認証):有効にすると、ユーザは認証データを知らなくてもログインできます。この場合は、管理者が認証データを提供する必要があります。表示されるオプションは選択したコネクションタイプに依存します。

- **ユーザ名:**ユーザが接続に使用するユーザ名を入力します。
- **パスワード:**ユーザが接続に使用するパスワードを入力します。

> **注 –** コネクションタイプ *Telnet* を使用する場合、セキュリティ上の理由から、Telnet サーバから送信されるバナーの長さが（パスワードプロンプトも含め）4096 文字を超えない場合のみ、自動ログインは機能します。バナーがそれ以上の文字数になると、自動ログインに失敗します。この場合は、バナーの長さを短くするか、手動のログインに切り替えます。

- **認証方式**（コネクションタイプが *SSH のみ*）:SSH の認証方式を選択します。選択したユーザ名に対する「*パスワード*」を提供するか、SSH 接続の「*SSH 秘密鍵*」を追加できます。

SSL ホスト証明書（コネクションタイプが *HTTPS のみ*）:宛先ホストを識別する SSL ホストのセキュリティ証明書を追加します。

- **SSL 証明書:**「フェッチ」ボタンをクリックして、選択した宛先ホストの証明書を自動的に追加します。

ホスト公開鍵（コネクションタイプが *SSH のみ*）:SSH ホストの公開鍵を追加します。

- **SSH 公開鍵:**「フェッチ」ボタンをクリックして、選択した宛先ホストの SSH 公開鍵を自動的に取得します。

許可ユーザ（ユーザポータル）:VPN ポータルコネクションの使用を許可するユーザまたはグループを追加します。初期状態では、1ユーザは 1つのコネクションを同時に利用することができます。ユーザが同時にセッションを共有したい場合、*共有セッション*チェックボックスの *詳細*セクション選択して下さい。

> **注 –** バックエンドメンバシップにグループを追加するとき、そのグループがユーザポータルにて許可されていることを確認して下さい。「*マネジメント > ユーザポータル > グローバル*」タブ、から選択するか、*全てのユーザを許可* か *特定のユーザのみ* もしくは明確にグループを追加。もし特定のグループメンバーのみにユーザポータルへの許可を与えた場合、そのグループへの許可は与えられないことになります。

コメント（任意）:説明などの情報を追加します。

4. **次の詳細設定を任意で行います。**

ポート:コネクションのポート番号を入力します。デフォルトでは、選択したコネクションタイプの標準ポートが選択されます。

プロトコルセキュリティ(コネクションタイプが *リモートデスクトップのみ*):リモートデスクトップセッションのセキュリティプロトコルを選択します。RDP、TLS または NLA (ネットワークレベル認証) から選択できます。選択する設定がサーバの設定に対応している必要があります。NLA を選択する場合は、上記の *自動ログイン*を有効にする必要があります。

共有セッション:ユーザに同時のコネクションと同じ画面の閲覧を許可する場合は、このオプションを選択します。

外部リソースを許可(コネクションタイプが *Webapp (HTTP/S)のみ*):このコネクション経由でアクセスを許可する追加のリソースを入力します。例えば、画像やその他のリソースが Web ページとは別のサーバに保管されている場合などに便利です。選択したホストまたはネットワーク範囲に対してポート 80 および 443 が許可されます。

5. **「*保存*」をクリックします。**
   新しいコネクションが「*コネクション*」リストに表示されます。
6. **コネクションを有効にします。**
   コネクションを有効にするには、トグルスイッチをクリックします。

   許可されたユーザがコネクションを使用できるようになります。これは、ユーザポータルの「*HTML5 VPN ポータル*」タブに表示されます。

接続を編集または削除するには、対応するボタンをクリックします。

16.6 Cisco VPN クライアント

Sophos UTM は、Cisco VPN クライアント経由の IPsec リモートアクセスをサポートします。Cisco VPN クライアントは、Cisco Systems の提供する実行可能形式プログラムです。これを使用すると、コンピュータのセキュリティを維持しながら VPN (*バーチャルプライベートネットワーク*)にリモート接続することができます。

16.6.1 グローバル

「*リモートアクセス > Cisco VPN クライアント > グローバル*」タブでは、Cisco VPN クライアント経由のリモートアクセスをセットアップするための基本オプションを設定することができます。

Sophos UTMを設定して Cisco VPN クライアント接続が許可されるようにするには、次の手順に従ってください。

1. **「*グローバル*」タブで、Cisco VPN クライアントを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*サーバ設定*」エリアが編集可能になります。

2. **次の設定を行います。**
   インタフェース: Cisco VPN クライアント接続に使用するインタフェースを選択します。

   サーバ証明書:サーバがクライアントに対して自らの身元を証明するために使用する証明書を選択します。

   プールネットワーク:接続クライアントに仮想ネットワークアドレスを割り当てるために、仮想ネットワークアドレスを選択するためのネットワークプールを選択します。デフォルトで「*VPN プール (Cisco)*」が選択されています。

   ユーザとグループ: Cisco VPN クライアント経由でUTMに接続することが許可されるユーザまたはグループ(あるいはその両方)を選択します。ただし、バックエンドメンバシップグループをボックスにドラッグすることはできません。この理由は、IPsec 設定時にユーザ証明書が必要であるにも関わらず、証明書はユーザが最初にログインに成功したときに初めて生成されるためです。

   ローカルネットワーク:VPN トンネル経由でアクセス可能にするローカルネットワークを選択します。

   自動ファイアウォールルール (オプション): このオプションを選択すると、この接続用のトラフィックを許可するファイアウォールルールを自動的に追加することができます。ルールは、接続が確立するとすぐに追加され、接続が無効になると削除されます。

3. **「*適用*」をクリックします。**
   設定が保存されます。

ライブログ

IPsec IKE デーモンログの接続ログを追跡するには、ライブログを使用します。ライブログには、接続の確立、維持、終了に関する情報が表示されます。

16.6.2 iOS デバイス

ユーザポータルで iOS デバイスに対し Cisco IPsec の自動設定を提供することができます。

ただし、「*グローバル*」タブの「*ユーザとグループ*」ボックスに追加されたユーザのみに対して、ユーザポータルサイトに設定ファイルが表示されます。iOS デバイスのステータスはデフォルトで有効になっています。

コネクション名:Cisco IPsec 接続を説明する名前を入力し、iOS デバイスのユーザがどの接続を確立しようとしているのか識別できるようにします。デフォルトの名前は、お客様の会社名の後に Cisco IPsec プロトコルが続いたものになります。

注 – 「*コネクション名*」はすべての iOS デバイス設定 (PPTP、L2TP over IPsec、Cisco VPN Client) で一意である必要があります。

ホスト名を上書き:システムのホスト名をクライアントがパブリックに解決できない場合は、ここにサーバのホスト名を入力して、これによって「*システムの DNS ホスト名*」の前の「*DynDNS ホスト名*」の内部設定を上書きします。

VPN 接続のオンデマンド確立:ロケーションがボックスのリスト内のホスト名またはドメインのいずれかと一致したときに接続を自動的に開始するには、このオプションを選択します。

- **ドメインまたはホストにマッチング**:オンデマンドで VPN 接続を確立するドメインまたはホスト名を入力します。例えばローカルイントラネットなどがここに入ります。
- **DNS 参照に失敗した場合のみ確立**:デフォルトでは、DNS 参照に失敗した場合のみ VPN 接続が確立されます。このオプションを選択しない場合は、ホスト名の解決に関係なく VPN 接続が確立されます。

接続する iOS デバイスが、「*グローバル*」タブに指定したサーバ証明書に表示されます。iOS デバイスは、この証明書の VPN ID がサーバのホスト名と一致しているかチェックし、異なる場合には接続を拒否します。サーバ証明書で VPN ID タイプに「*識別名*」を使用している場合、代わりに「*一般名*」フィールドが使用されます。サーバ証明書がこれらの制約を満たしていることを確認する必要があります。

iOS デバイスの自動設定を無効にするには、トグルスイッチをクリックします。

トグルスイッチがグレーに変わります。

16.6.3 デバッグ

IKE デバッグ

「*IKE デバッグ*」セクションで IKE デバッグオプションを設定できます。どのタイプの IKE メッセージまたは通信についてデバッグ出力を作成するかはチェックボックスで選択します。

注 – 「*IKE デバッグ*」セクションは、「*サイト間 VPN IPsec*」、「*リモートアクセス IPsec*」、「*L2TP over IPsec*」、および「*Cisco VPN クライアント*」メニューの「*デバッグ*」タブで同じものが使用されています。

以下のフラグをログできます。

- **コントロールフロー:**IKE ステートのコントロールメッセージを表示します。
- **アウトバウンドパケット:**送信 IKE メッセージのコンテンツを表示します。
- **インバウンドパケット:**受信 IKE メッセージのコンテンツを表示します。
- **カーネルメッセージ:**カーネルとの通信メッセージを表示します。
- **冗長構成 (HA)**その他の HA ノードとの通信を表示します。

16.7 詳細

「*リモートアクセス > 詳細*」ページでは、リモートアクセスクライアントの詳細設定を行うことができます。ここで入力するDNS サーバとWINS サーバの IP アドレスは、ゲートウェイへの接続の確立時にリモートアクセスクライアントを使用するために提供され、これによってドメインの完全な名前解決が実現します。

DNS サーバ:組織の DNS サーバを最大 2台指定します。

WINS サーバ:組織の WINS サーバを最大 2台指定します。WINS *(Windows インターネットネーミングサービス)*とは、マイクロソフトが Windows OS に実装した NBNS *(NetBIOSネームサーバ)*です。DNS がドメイン名を対象にしているように、WINS は NetBIOS 名を対象にしてホスト名とIP アドレスを一元的にマッピングします。

ドメイン名:組織の *完全修飾ドメイン名* (FQDN)を入力します。完全修飾ドメイン名とは、DNS ツリー階層でのノードの絶対位置を指定する明瞭なドメイン名です(`intranet.example.com` など)。

注 – PPTP およびL2TP over IPsec の場合、ドメイン名は自動的に配信 できず、クライアント側で設定する必要があります。
*Cisco VPN クライアント*を使用する iOS デバイスでは、上で指定した DNS サーバが指定ドメインに属するホストの解決にのみ使用されます。

16.8 証明書管理

「*サイト間 VPN > 証明書管理*」メニューと「*リモートアクセス > 証明書管理*」メニューには、同じ設定オプションが含まれています。これらの設定オプションを使用すると、Sophos UTMのすべての証明書関連オプションを管理することができます。たとえば、X.509 証明書の作成またはインポートや、CRL *(証明書失効リスト)*のアップロードなどを行うことができます。

16.8.1 証明書

*「サイト間 VPN」>「証明書管理」>「証明書」*を参照してください。

16.8.2 認証局（CA）

「*「サイト間 VPN > 証明書管理 > CA」*を参照してください。

16.8.3 証明書失効リスト(CRL)

*「サイト間 VPN」>「証明書管理」>「証明書失効リスト（CRL）」*を参照してください。

16.8.4 詳細

「*サイト間 VPN > 証明書管理 > 詳細」*を参照してください。

17 ログとレポート

この章では、Sophos UTMのログおよびレポート機能について説明します。

Sophos UTM は、各種システムおよびネットワーク保護イベントを継続的に記録することにより、豊富なログ機能を提供します。詳細な監査証跡により、過去と現在のさまざまなネットワークアクティビティに関する分析が実現し、潜在的なセキュリティ上の脅威を特定したり、発生している問題のトラブルシューティングを行うことができます。

Sophos UTMのレポート機能は、現在のログデータを収集し、それをグラフ形式で表示することで、管理対象デバイスのリアルタイム情報を提供します。

WebAdmin の「*ログパーティションステータス*」ページは、ディスクの残容量、フィルアップレート（使用量増加速度）についての情報や、過去 4週間のログパーティションの使用状況を示すヒストグラムなど、Sophos UTMユニットのログパーティションのステータスを示します。フィルアップレートは、測定地点と開始地点の差分を経過時間で割って計算するため、当初は値がやや不正確になりますが、システムの稼働時間が長くなればなるほど精度が増します。

この章では、次のトピックについて説明します。

- ログファイルの閲覧
- ハードウェア
- ネットワーク使用率
- ネットワークプロテクション
- Webプロテクション
- Eメールプロテクション
- リモートアクセス
- Webサーバプロテクション
- エグゼクティブレポート
- ログ設定
- レポート設定

レポーティンググラフ

Sophos UTM レポーティンググラフを折れ線グラフや円グラフで表示します。対話的な性質上、これらのグラフでは情報にきめ細かくアクセスすることが可能となっています。

折れ線グラフ

折れ線グラフへの対話的操作が簡単です。マウスのカーソルをグラフ上に置くと、大きなドット(点)が表示され、グラフのその部分の詳細な情報が表示されます。このドットは、グラフの線に沿って移動します。マウスのカーソルを移動すると、ドットもそれに従って移動します。グラフに何本かの線がある場合、ドットはマウスカーソルの移動に従って線の間を移動します。さらに、ドットの色は、それが表示している情報がどの線に関連するかによって変わるため、線が互いに近接している場合に役立ちます。

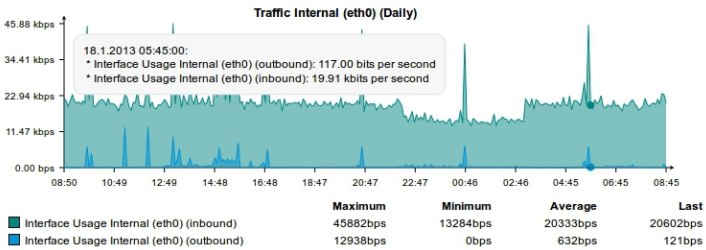

Figure 27 レポーティング:折れ線グラフの例

円グラフ

折れ線グラフと同様に、円グラフも対話的な操作を行うことができます。マウスのカーソルを円グラフの一部に置きます。すると、その部分は円グラフの他の部分から即座に切り離され、その部分の詳細な情報がツールヒントに表示されます。

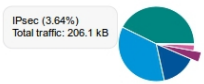

Figure 28 レポーティング:円グラフの例

17.1 ログファイルの閲覧

「*ログとレポート > ログファイルの閲覧*」メニューで、各種ログファイルを表示および検索できます。

17.1.1 今日のログファイル

「*ログとレポート > ログファイルの閲覧 > 今日のログファイル*」タブで、現在のすべてのログに容易にアクセスできます。

このタブでは、すべてのログファイルに適用できるさまざまな作業を実行できます。次の作業を実行できます。

- **ライブログ:**ポップアップウインドウが開き、リアルタイムでログファイルを表示できます。新しいアクティビティが発生すると、リアルタイムでログファイルに新しい行が追加されます。「*自動スクロール*」を選択すると、ポップアップウインドウが自動的スクロールダウンして、常に最新のログが表示されます。さらに、ポップアップウインドウにはフィルタテキストボックスも含まれており、これによって新しいログの表示ををフィルタに一致するレコードだけに制限できます。
- **表示:**ポップアップウィンドウが開き、現在の状態のログファイルが表示されます。
- **クリア:**ログファイルのコンテンツを削除します。

テーブル下部のドロップダウンリストを使用して、選択したログファイルを `zip` ファイル形式でダウンロードしたり、それらのコンテンツを同時に削除したりできます。

17.1.2 アーカイブログファイル

「*ログとレポート > ログファイルの閲覧 > アーカイブログファイル*」タブで、ログファイルアーカイブを管理することができます。すべてのログファイルはデイリーベースでアーカイブされます。アーカイブしたログファイルにアクセスするには、ログが書き込まれているSophos UTMのサブシステムと年月を選択します。

選択に一致したすべての利用できるログファイルが年代順に表示されます。アーカイブしたログファイルは、閲覧したり、`zip` ファイル形式でダウンロードできます。

テーブル下部のドロップダウンリストを使用して、選択したログファイルを`zip`ファイル形式でダウンロードしたり同時に削除したりすることができます。

17.1.3 ログファイルの検索

「*ログとレポート > ログファイルの閲覧 > ログファイルの検索*」タブで、さまざまな期間のローカルログファイルを検索できます。最初に、検索するログファイルを選択し、次に検索する語句を入力して、検索期間を選択します。「*期間を選択*」リストから「*カスタム期間*」を選択した場合は、開始日と終了日を指定できます。「*検索開始*」ボタンをクリックすると、ポップアップウインドウにクエリ結果が表示されます。ブラウザによっては、WebAdmin 用にポップアップウインドウを許可する必要があります。

17.2 ハードウェア

「*ログとレポート > ハードウェア*」メニューには、さまざまな期間におけるハードウェアコンポーネントの使用状況に関する概要的な統計が表示されます。

17.2.1 デイリー

「*ハードウェア > デイリー*」タブは、次のハードウェアコンポーネントに関する過去 24時間の統計概観を示します。

- CPU の使用状況
- メモリ/スワップの使用状況
- パーティションの使用状況

CPU の使用状況:ヒストグラムに、現在のプロセッサ使用状況 (%) が表示されます。

メモリ/スワップの使用状況:メモリとスワップの使用状況 (%)。スワップの使用状況は、システム構成によって大きく異なります。侵入防御やプロキシサーバなどのサービスをアクティブにすると、メモリの使用率が高くなります。システムのメモリが不足すると、スワップスペースが使用されるようになり、システム全体のパフォーマンスが低下します。スワップスペースの使用はできるだけ低く抑える必要があります。このためには、システムで利用できるメモリの合計容量を増やします。

パーティションの使用状況:選択されたパーティションの使用状況 (%)。すべてのチャートには3つのグラフが表示され、それぞれが1つのハードディスクドライブパーティションを示します。

- **ルート:**ルートパーティションとは、Sophos UTMのルートディレクトリがあるパーティションです。このパーティションには、更新パッケージとバックアップも保存されます。

- **ログ:**ログパーティションとは、ログファイルとレポーティングデータが保存されるパーティションです。このパーティションの容量が不足している場合、「*ログとレポート > ログ設定 > ローカルログ*」で設定を調整してください。
- **ストレージ:**ストレージパーティションとは、プロキシサービスがデータを保存するパーティションであり、Web フィルタ用の画像、SMTP プロキシ用のメッセージ、隔離メールなどがここに保存されます。さらに、データベース、一時データ、設定ファイルも保存されます。

17.2.2 ウィークリー

「*ハードウェア > ウィークリー*」タブは、選択されたハードウェアコンポーネントに関する過去7日間の概要的な統計を示します。ヒストグラムについては、「*デイリー*」のセクションを参照してください。

17.2.3 マンスリー

「*ハードウェア > マンスリー*」タブは、選択されたハードウェアコンポーネントに関する過去4週間の概要的な統計を示します。ヒストグラムについては、「*デイリー*」のセクションを参照してください。

17.2.4 年次

「*ハードウェア > 年次*」タブは、選択されたハードウェアコンポーネントに関する過去 12か月間の概要的な統計を示します。ヒストグラムについては、「*デイリー*」のセクションを参照してください。

17.3 ネットワーク使用状況

「*ログとレポート > ネットワーク使用状況*」メニューのタブには、さまざまな期間内にSophos UTMの各インタフェースを通過したトラフィックに関する概要的な統計が表示されます。各チャートのデータは、次の単位を使用して示されます。

- u (マイクロ、10^{-6})
- m (ミリ、10^{-3})
- k (キロ、10^{3})
- M (メガ、10^{6})
- G (ギガ、10^{9})

10^{-18}～10^{8} の範囲内でスケーリング可能です。

17.3.1 デイリー

「*ネットワーク使用状況 > デイリー*」タブには、設定されている各インタフェースを通過するトラフィックに関する過去24時間の概要的な統計が表示されます。

各ヒストグラムには、次の2つのグラフが表示されます。

- **受信:**該当インタフェースでの平均受信トラフィック(bps単位)。
- **送信:**該当インタフェースでの平均送信トラフィック(bps単位)。

「*同時接続数*」チャートは、同時接続の合計を示します。

17.3.2 ウィークリー

「*ネットワーク使用状況 > ウィークリー*」タブには、設定されている各インタフェースを通過するトラフィックに関する過去 7日間の概要的な統計が表示されます。ヒストグラムについては、「*デイリー*」のセクションを参照してください。

17.3.3 マンスリー

「*ネットワーク使用状況 > マンスリー*」タブには、設定されている各インタフェースを通過するトラフィックに関する過去4週間の概要的な統計が表示されます。ヒストグラムについては、「*デイリー*」のセクションを参照してください。

17.3.4 年次

「*ネットワーク使用状況 > イヤリー*」タブには、設定されている各インタフェースを通過するトラフィックに関する過去12か月の概要的な統計が表示されます。ヒストグラムについては、「*デイリー*」のセクションを参照してください。

17.3.5 帯域使用状況

「*ネットワーク使用状況 > 帯域使用状況*」タブには、デバイスから転送されたネットワークトラフィック、デバイスに転送されたネットワークトラフィック、デバイスを経由して転送されたネットワークトラフィックについての包括的なデータが表示されます。

最初のドロップダウンリストから、表示するデータのタイプを選択します(例: *上位クライアント*や*上位サービス*、*クライアント別*など)。必要なエントリを選択し、追加でボックスが表示される場合は、

該当するすフィルタの条件を指定します。または、下部にあるドロップダウンリストを使用して、時刻によってエントリをフィルタリングできます。フィルタを適用するには、そのつど「*更新*」ボタンをクリックします。

結果の表の「*クライアント別/サーバ別*」ビューで IP またはホスト名をクリックすると、これは自動的に「*クライアント別の上位サービス*」ビューのフィルタとして使用されます。後でこれを「*サーバ別の上位サービス*」ビューに切り替えることや、IP/ネットワークやネットワーク範囲（`192.168.1.0/24`、`10/8` など）を手動で指定して「*更新*」ボタンをクリックし、これらの設定を確定することができます。
「*サービス別*」ビューでは、プロトコルとサービスをコンマで区切って入力することができます（*TCP,SMTP*、*UDP,6000* など）。プロトコルを指定しないと、TCP が使用されます（*HTTP* も有効です）。デフォルトでは、1ページあたり 20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。「*行数*」ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

上位アプリケーション/上位アプリケーショングループ:アプリケーションコントロールがオフの場合、ネットワークトラフィックは「未分類」と表示されます。アプリケーションコントロールが有効な場合、ネットワークトラフィックはタイプで表示されます（例:「WebAdmin」、「NTP」、「facebook」）。アプリケーションコントロールに関する詳細は、「*Web プロテクション > アプリケーションコントロール*」の章を参照してください。

タブ右上隅の対応するアイコンをクリックすると、データを PDF あるいは Excel 形式でダウンロードできます。レポートは、現在選択されているビュー（表示）から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

トラフィックのラベル *IN* と *OUT* は、視点に応じて異なります。プロキシモードで実行している場合、クライアントは（透過モードであっても）UTMでポート `8080` に接続するため、このクライアントから送信されたデータ（要求）は内部インタフェースにおいて *受信*トラフィックとなり、クライアント宛てに送信されたデータ（応答）は *送信*トラフィックとなります。

表の列のヘッダをクリックすると、すべてのデータを並べ替えることができます。たとえば、すべてのホストを受信トラフィック別にソートする場合、表の見出しで「*IN*」をクリックします。これにより、受信トラフィックが最も多く発生しているホストが先頭に表示されます。トラフィックのデータ量はキビバイト（KiB）およびメビバイト（MiB）単位で表示されます。いずれも、コンピュータの記憶容量を示す 2 の累乗単位です（例: 1キビバイト = 2^{10}バイト = 1024バイト）。

17.4 ネットワークプロテクション

「*ログとレポート > ネットワークプロテクション*」メニューのタブには、Sophos UTMによって検出された関連ネットワークプロテクションイベントについての概要的な統計が表示されます。

17.4.1 デイリー

「*ネットワークプロテクション > デイリー*」タブは、次のイベントに関する過去 24時間の統計概観を示します。

- ファイアウォール違反
- 侵入防御統計

ファイアウォール違反:ドロップまたは拒否されたすべてのデータパケットは、ファイアウォール違反としてカウントされます。ファイアウォール違反の回数は、5分間の枠内で計算されます。

IPS統計:すべてのグラフには、次の 2つのグラフが表示されます。

- **アラートイベント:**侵入アラートをトリガしたデータパケットの数。
- **ドロップイベント:**侵入防御システムによってドロップされたデータパケットの数。

17.4.2 ウィークリー

「*ネットワークプロテクション > ウィークリー*」タブには、過去 7日間以内に発生したファイアウォール違反および侵入防御イベントに関する概要的な統計が表示されます。ヒストグラムについては、「デイリー」のセクションを参照してください。

17.4.3 マンスリー

「*ネットワークプロテクション > マンスリー*」タブには、過去 4週間以内に発生したファイアウォール違反および侵入防御イベントに関する概要的な統計が表示されます。ヒストグラムについては、「デイリー」のセクションを参照してください。

17.4.4 年次

「*ネットワークプロテクション > イヤリー*」タブには、過去 12か月以内に発生したファイアウォール違反および侵入防御イベントに関する概要的な統計が表示されます。ヒストグラムについては、「デ

イリー」のセクションを参照してください。

17.4.5 ファイアウォール

「*ネットワークプロテクション > ファイアウォール*」タブには、ファイアウォールアクティビティに関する包括的なデータが、送信元 IP、送信元ホスト、受信パケット数、サービス数に従って分類されて表示されます。

注 – TTL が 1以下のパケットはログに記録されずにドロップされます。

最初のドロップダウンリストから、表示するデータのタイプを選択します(例: *上位送信元ホスト*や*上位サービス*、*宛先別*など)。必要なエントリを選択し、追加でボックスが表示される場合は、該当するすフィルタの条件を指定します。または、下部にあるドロップダウンリストを使用して、時刻によってエントリをフィルタリングできます。フィルタを適用するには、そのつど「*更新*」ボタンをクリックします。

結果の表で IP またはホスト名をクリックすると、「*上位サービス*」ビューのフィルタとして自動的に使用されます。IP/ネットワークやネットワーク範囲(`192.168.1.0/24`、`10/8` など)を手動で指定して、「*更新*」ボタンを押し、これらの設定を使用することができます。
「*サービス別*」ビューでは、プロトコルとサービスをコンマで区切って入力することができます(*TCP,SMTP*、*UDP,6000* など)。

デフォルトでは、1ページあたり 20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。「*行数*」ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

タブ右上隅の対応するアイコンをクリックすると、データを PDF あるいは Excel 形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

表の列のヘッダをクリックすると、すべてのデータを並べ替えることができます。

17.4.6 IPS

「*ネットワークプロテクション > IPS*」タブには、ネットワークでの侵入防御アクティビティに関する包括的なデータが表示されます。

最初のドロップダウンリストから、表示するデータのタイプを選択します(例: *上位送信元ホスト*や*上位宛先*、*送信元別*など)。必要なエントリを選択し、追加でボックスが表示される場合は、該当するすフィルタの条件を指定します。または、下部にあるドロップダウンリストを使用して、時刻によって

エントリをフィルタリングできます。フィルタを適用するには、そのつど「*更新*」ボタンをクリックします。

デフォルトでは、1ページあたり20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。「*行数*」ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

表の列のヘッダをクリックすると、すべてのデータを並べ替えることができます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

17.5 Webプロテクション

「*ログとレポート*>*Webプロテクション*」メニューのタブには、最もアクティブなWebユーザと最もよく表示されているWebサイトに関する概要的な統計が表示されます。

17.5.1 Web使用状況レポート

「*ログとレポート*>*Webプロテクション*>*Web使用状況レポート*」ページは、ネットワークトラフィックやユーザのWeb使用状況を確認するための強力なツールです。一見するとこのページは非常に難解ですが、使用してみて結果を調べることから始めてみましょう。

ページ構成

ヘッダバー

まず、次の要素から構成されているヘッダバーがあります。

- **ホーム:**このアイコンを使用して、クリックやフィルタをすべてクリアして最初の状態に戻すことができます。
- **前へ/次へ:**これらのアイコンを使用して、変更や設定の履歴を前へ(または後ろへ)移動することができます。一般的なWebブラウザと同様に機能します。
- **閲覧可能なレポート:**このドロップダウンリストには、保存されたレポート(もしあれば)を含む、利用可能なすべてのレポートタイプが含まれます。これはデフォルトで「*サイト*」に設定されています。「*Web使用状況レポート*」ページの結果テーブルは、このレポートタイプ設定に直接依存しています。

注 – フィルタを使用してレポートを次々にクリックすると、「*閲覧可能なレポート*」設定が自動的に変化するのを確認できます。これは常に、最新のレポート基準が反映されます。

標準:レポートタイプは複数あります。詳細は以下を参照してください。

保存済み Web レポート:ここでは、過去に作成した、保存された Web レポートを選択できます。

- **削除:**保存された Web レポートを削除するには、このアイコンをクリックします。標準レポートは削除できません。
- **保存:**現在のビューを保存して、後日このビューに簡単にアクセスできるようにするには、このアイコンをクリックします。これは「*利用可能なレポート*」ドロップダウンリストに保存されます。「*レポートの送信*」チェックボックスにチェックを入れると、このレポートを受信すべきメール受信者を 1人以上入力することができます。また、保存されたレポートを定期的に受信することもできます。詳しくは「*スケジュールされたレポート*」を参照してください。

フィルタバー

次に、次の要素から構成されているフィルタバーがあります。

- **プラス (+):**このアイコンをクリックして、追加のフィルタを作成します。詳細は以下を参照してください。
- **件数:**ドロップダウンリストを使用して、テーブルに表示される結果を減らすことができます。結果を、上位 10件、50件、100件の結果に制限することができます。
- **時刻:**ドロップダウンリストを使用して、テーブルに表示される結果を、特定の時間枠内の結果に絞り込むか広げることができます。「*カスタム*」タイムフレームを選択すると、独自の時間枠を指定できます。
- **部門:**ドロップダウンリストを使用して、テーブルに表示される結果を、指定した部門に絞り込むことができます。部門は「*部門*」ページで作成できます。

結果テーブル

最後に、結果テーブルがあります。ここに表示される結果は、第一に、選択したレポートタイプに依存し(「*利用可能なレポート*」リストに常に反映)、第二に、定義したフィルタに依存します。

注 – 匿名化を有効にすると、ユーザは名前や IP アドレスで表示される代わりに、数値で列挙されます。

レポートタイプに応じて、テーブルには異なる情報が表示されます。

	ユーザ	カテゴリ	サイト	ドメイン	URL	上書き
#	✔	✔	✔	✔	✔	✔
トラフィック	✔	✔	✔	✔	✔	
%	✔	✔	✔	✔	✔	
期間	✔		✔			
ページ	✔	✔	✔			
リクエスト	✔	✔	✔	✔	✔	
ユーザ						✔
サイト						✔
カテゴリ*					✔	✔
アクション*					✔	✔
理由*					✔	✔
情報*					✔	✔

*=これらのセルをクリックして、情報をさらにドリルダウンできます。

#:発生したトラフィックに関する順位。

トラフィック:発生したトラフィックのサイズ。

%:トラフィック全体に対する割合。

期間:ユーザが Web サイトに滞在した時間。

ページ:要求されたページ数

要求:カテゴリ、サイト、ドメイン、または URL 別の要求数。

ユーザ:ブロックを回避したユーザ名。匿名化を有効にすると、*user_#*が表示されます。

サイト:ブロックが回避されたサイト。

カテゴリ:ある URL が属するすべてのカテゴリが表示されます。カテゴリが複数存在する場合、カテゴリをクリックすると小さいダイアログフィールドが開き、いずれかのカテゴリを選択できます。このカテゴリに基づいてフィルタが作成されます。

アクション: Web サイトがクライアントに配信されたか(*配信済み*)、アプリケーションコントロールルールによって*ブロック*されたか、またはブロックの回避機能を使用してユーザがブロックされたページへアクセスしたか(*オーバーライド*)を表示します。

理由: Web サイト要求がブロックまたはオーバーライドされた理由を表示します。例:ユーザが `msi` ファイルのダウンロードを試行し、ファイル転送を禁止するアプリケーションコントロールルールが

あった場合、セルに理由が「msi」と表示されます。オーバーライドされたページの場合、ユーザによって入力された理由が表示されます。

情報:利用可能な場合、このセルには Web サイト要求がブロックされた理由を示す追加情報が表示されます(例:ファイルダウンロードが拡張子に基づいてブロックされた場合、セルには「拡張子」と表示されます)。

フィルタの定義

フィルタは、結果テーブルに表示される情報をドリルダウンするために使用されます。2とおりの定義方法があります。フィルタバーの「+」アイコンをクリックするか、テーブルをクリックします。

「+」アイコンを使用する場合:フィルタバーで緑の「+」アイコンをクリックすると、フィールドが 2つある小さいフィルタバーが表示されます。1番目のフィールドのドロップダウンリストを使用すると、レポートタイプを選択できます(「*カテゴリ*」など)。2番目のフィールドを使用すると、選択したレポートタイプの値を選択するか入力することができます(例:「*カテゴリ*」を選んだ場合、「*成人向けトピック*」など)。「*保存*」をクリックしてフィルタを保存し、結果テーブルに適用します。

テーブルを使用する場合:テーブルをクリックし、クリックしたアイテムに複数のレポートタイプがある場合は、「*レポート方向*」が開きます。表示されたいずれかのオプションをフィルタ用に選択する必要があります。「*レポート方向*」ウィンドウを閉じると、関連フィルタが作成され、フィルタバーに表示されます。結果テーブルに、新たにフィルタされた結果が表示されます。
例:「*Web 使用状況 レポート*」のデフォルトレポートは「*サイト*」です。結果テーブルで、任意の行をクリックします(例:「amazon.com」)。「*レポート方向*」ウィンドウが開き、3つのオプションが提示されます。サイトの*ドメイン*に関する情報、サイトを訪問した*ユーザ*に関する情報、サイトが属する*カテゴリ*に関する情報のいずれかを参照することができます。複数のユーザが「amazon.com」を訪問したことがわかりました。さらに詳細を確認するために、「ユーザ」ボックスをクリックします。ウィンドウが閉じます。ヘッダバーではレポートタイプが「ユーザ」に変わり、フィルタバーでは「ユーザ」の結果テーブルが選択したサイト(「amazon.com」)によってフィルタされたことを確認できます。したがって、テーブルにはこのサイトを訪問したすべてのユーザと、これらのセッションに関する追加情報が表示されます。

注 – 一部のテーブルセルには独自のフィルタがあるため(上の「*結果テーブル*」セクションでアスタリスク(*)の付いたアイテム)、クリックしたテーブル行によって結果が異なる場合があります。

17.5.2 検索エンジンレポート

「*ログとレポート > Web プロテクション > 検索エンジンレポート*」ページには、ユーザが使用している検索エンジンやユーザが行った検索に関する情報が表示されます。一見するとこのページは非常

に難解ですが、使用してみて結果を調べることから始めてみましょう。

ページ構成

ヘッダバー

まず、次の要素から構成されているヘッダバーがあります。

- **ホーム:**このアイコンを使用して、クリックやフィルタをすべてクリアして最初の状態に戻すことができます。
- **前へ/次へ:**これらのアイコンを使用して、変更や設定の履歴を前へ(または後ろへ)移動することができます。一般的なWebブラウザと同様に機能します。
- **閲覧可能なレポート:**このドロップダウンリストには、保存されたレポート(もしあれば)を含む、利用可能なすべてのレポートタイプが含まれます。これはデフォルトで「*検索*」に設定されています。「*検索エンジンレポート*」ページの結果テーブルは、このレポートタイプ設定に直接依存しています。

  注 – フィルタを使用してレポートを次々にクリックすると、「*閲覧可能なレポート*」設定が自動的に変化するのを確認できます。これは常に、最新のレポート基準が反映されます。

  標準:レポートタイプは3種類あります。詳細は以下を参照してください。

  保存された検索エンジンレポート:ここでは、過去に作成した、保存された検索エンジンレポートを選択できます。
- **削除:**保存された検索エンジンレポートを削除するには、このアイコンをクリックします。標準レポートは削除できません。
- **保存:**現在のビューを保存して、後日このビューに簡単にアクセスできるようにするには、このアイコンをクリックします。これは「*利用可能なレポート*」ドロップダウンリストに保存されます。「*レポートの送信*」チェックボックスにチェックを入れると、このレポートを受信すべきメール受信者を1人以上入力することができます。また、保存されたレポートを定期的に受信することもできます。詳しくは「*スケジュールされたレポート*」を参照してください。

フィルタバー

次に、次の要素から構成されているフィルタバーがあります。

- **プラス(+):**このアイコンをクリックして、追加のフィルタを作成します。詳細は以下を参照してください。

- **件数:**ドロップダウンリストを使用して、テーブルに表示される結果を減らすことができます。結果を、上位 10件、50件、100件の結果に制限することができます。
- **時刻:**ドロップダウンリストを使用して、テーブルに表示される結果を、特定の時間枠内の結果に絞り込むか広げることができます。「*カスタム*」タイムフレームを選択すると、独自の時間枠を指定できます。
- **部門:**ドロップダウンリストを使用して、テーブルに表示される結果を、指定した部門に絞り込むことができます。部門は「*部門*」ページで作成できます。

結果テーブル

最後に、結果テーブルがあります。ここに表示される結果は、第一に、選択したレポートタイプに依存し(「*利用可能なレポート*」リストに常に反映)、第二に、定義したフィルタに依存します。次のレポートタイプを使用できます。

- **検索:**ユーザが使用した検索文字列を表示します。
- **検索エンジン:**ユーザが使用した検索エンジンを表示します。
- **ユーザの検索:**検索を行ったユーザを表示します。

注 – 匿名化を有効にすると、ユーザは名前や IP アドレスで表示される代わりに、数値で列挙されます。

それぞれのレポートタイプに対して、テーブルには以下の情報が表示されます。

#:頻度に関する順位。

要求:検索文字列、検索エンジン、ユーザ別の要求回数。

%:検索全体に対する割合。

フィルタの定義

フィルタは、結果テーブルに表示される情報をドリルダウンするために使用されます。2とおりの定義方法があります。フィルタバーの「+」アイコンをクリックするか、テーブルをクリックします。

「+」アイコンを使用する場合:フィルタバーで緑の「+」アイコンをクリックすると、フィールドが 2つある小さいフィルタバーが表示されます。1番目のフィールドのドロップダウンリストを使用すると、レポートタイプを選択できます(「*検索エンジン*」など)。2番目のフィールドを使用すると、選択したレポートタイプの値を選択するか入力することができます(例:「*検索エンジン*」を選んだ場合、「*Google (google.com)*」など)。「*保存*」をクリックしてフィルタを保存し、結果テーブルに適用します。

テーブルを使用する場合:テーブルをクリックし、クリックしたアイテムに複数のレポートタイプがある場合は、「*レポート方向*」が開きます。表示されたいずれかのオプションをフィルタ用に選択する必要があります。「*レポート方向*」ウィンドウを閉じると、関連フィルタが作成され、フィルタバーに表示されます。結果テーブルに、新たにフィルタされた結果が表示されます。
例:「*検索エンジンレポート*」のデフォルトレポートは「*検索*」です。結果テーブルで、任意の行をクリックします(例:「天気」)。「*レポート方向*」ウィンドウが開き、2つのオプションが提示されます。検索に対して使用された検索エンジンに関する情報を表示するか(「*検索エンジン*」)、この文字列を検索したユーザに関する情報を表示します(「*ユーザ検索*」)。複数のユーザが「天気」について検索したことがわかりました。さらに詳細を確認するために、「*ユーザ検索*」ボックスをクリックします。ウィンドウが閉じます。ヘッダバーでレポートタイプが「*ユーザ検索*」に変わり、フィルタバーで「*ユーザ検索*」の結果テーブルが選択した検索文字列(「天気」)によってフィルタされたことを確認できます。したがって、テーブルには「天気」について検索したすべてのユーザと、これらの検索に関する追加情報が表示されます。

17.5.3 部門

「*ログとレポート > Web プロテクション > 部門*」ページでは、ユーザまたはホストおよびネットワークを仮想部門にグループ化することができます。次に、これらの部門を使用して Web 使用状況レポートや検索エンジンレポートをフィルタすることができます。

部門を作成するには、次の手順に従います。

1. **「*部門*」タブで、「*部門の追加*」をクリックします。**
   「*新規部門の追加*」ダイアログボックスが開きます。
2. **名前を入力します。**
   「*名前*」フィールドに、部門を説明する名前を入力します。
3. **ユーザまたはホスト/ネットワークを追加します。**
   部門の定義には、ユーザとホスト/ネットワークのいずれかしか含めることができず、両方を同時に含めることはできません。
   - **ユーザ:**この部門に加えるユーザを 1人以上ボックスに追加します。
   - **ホスト/ネットワーク:**この部門に加えるホストまたはネットワークを 1つ以上ボックスに追加します。

   コメント(任意):説明などの情報を追加します。
4. **「*保存*」をクリックします。**
   新しい部門が「*部門*」リストに表示されます。

部門を編集、削除、または複製するには、対応するボタンをクリックします。

部門の使用について詳しくは、「*Web 使用状況レポート*」と「*検索エンジンレポート*」のセクションを参照してください。

17.5.4 スケジュールレポート

「*ログとレポート > Web プロテクション > スケジュールレポート*」ページでは、定期的にメールで送信したい保存済みレポートを定義することができます。スケジュールレポートを作成するためには、あらかじめ保存済みのレポートが少なくとも 1つ必要です(レポートの保存については、「*Web 使用状況レポート*」または「*検索エンジンレポート*」のセクションを参照)。

スケジュールレポートを作成するには、次の手順に従います。

1. **「スケジュールレポート」タブで、「スケジュールレポートの追加」をクリックします。**
   「*新規スケジュールレポートの追加*」ダイアログボックスが開きます。
2. **次の設定を行います。**
   名前:スケジュールレポートを説明する名前を入力します。

   間隔:ドロップダウンリストから、レポートを送信する間隔を選択します。

   レポート:保存されたすべてのレポートがここに表示されます。選択した間隔で送信する各レポートの前にあるチェックボックスにチェックを入れてください。

   受信者:選択したレポートを受信する受信者をボックスに追加します。インポートボタンを使用して受信者のリストを追加することができます。

   コメント(任意):説明などの情報を追加します。
3. **「保存」をクリックします。**

   新しいスケジュールされたレポートが「*スケジュールレポート*」リストに表示されます。

スケジュールレポートを編集、削除、または複製するには、対応するボタンをクリックします。スケジュールレポート自体を削除せずにレポートの送信を無効化するには、レポートのトグルスイッチを使用します。

17.5.5 アプリケーションコントロール

「*ログとレポート > Web プロテクション > アプリケーションコントロール*」ページには、様々な期間における最もアクティブな送信元、最も訪問が頻繁な宛先、最も人気の高いアプリケーションについての総合的な統計が表示されます。

最初のドロップダウンリストから、表示するデータのタイプを選択します(例: *上位送信元*や*上位アプリケーション*など)。必要なエントリを選択し、追加でボックスが表示される場合は、該当するす

フィルタの条件を指定します。または、下部にあるドロップダウンリストを使用して、時刻によってエントリをフィルタリングできます。フィルタを適用するには、そのつど「*更新*」ボタンをクリックします。

デフォルトでは、1ページあたり20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。「*行数*」ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

表の列のヘッダをクリックすると、すべてのデータを並べ替えることができます。

最もアクティブな送信元はすぐには表に表示されず、セッションタイムアウトの発生後に表示されます。たとえば、特定クライアント(ユーザ名またはIPアドレス)が5分間Webサーフィンを停止したとします。この場合、UTMはこのサーフィンセッションを「デッド(dead)」と判断し、最もアクティブな送信元リストに表示する前にデータベースに送ります。

さらに、「*アプリケーション別*」あるいは「*送信元別*」を使用したレポートも選択できます。続いて、フィルタフィールドが表示されます。ここに、求めるアプリケーションや送信元を入力し、「*更新*」をクリックして設定を確認する必要があります。表には、指定したアプリケーションまたは送信元でフィルタされた結果が表示されます(もしあれば)。
パーセント記号(%)をワイルドカードとして使用できます。キーワード末尾にパーセント記号を付けた場合は、完全一致または部分一致を検索するようにSophos UTMに指示することになります。フィルタフィールドでは大文字と小文字が区別されます。例:「*アプリケーション*」フィールドに「Google%」と入力すると、表には「Google Safe Browsing」、「Google Analytics」、「Google」などが表示されますが、「google」は表示され*ません*。

17.5.6 非匿名化

「*Webプロテクション>非匿名化*」タブは、匿名化が有効になっている場合のみアクセス可能です(「*ログとレポート>レポーティング設定>匿名化*」を参照)。

ここでは、Webプロテクションレポートに関する特定ユーザの匿名化をやめることができます。次の手順で実行します。

1. **両方のパスワードを入力します。**
   匿名化を有効にするために指定した1番目と2番目のパスワードを入力します。

2. **非匿名化にするユーザを追加します。**
   「*ユーザの非匿名化*」ボックスに、非匿名にするユーザのユーザ名を追加します。

3. **「*適用*」をクリックします。**
   設定が保存されます。

17.6 Eメールプロテクション

「*ログとレポート > Eメールプロテクション*」メニューのタブには、メールフロー、メール使用状況、およびEメールプロテクションについての概要的な統計が表示されます。

17.6.1 使用状況グラフ

「*Eメールプロテクション > 使用状況グラフ*」タブには、さまざまな時間枠内にUTMを通過したメールフローの概要的な統計が表示されます。

- デイリー
- ウィークリー
- マンスリー
- 年次

17.6.2 メール使用状況

「*Eメールプロテクション > メール使用状況*」タブには、さまざまな時間帯で最もアクティブに使用されたメールアドレスやアドレスドメインに関する包括的な統計が表示されます。

最初のドロップダウンリストから、表示するデータのタイプを選択します（例: *上位送信者*や*上位ドメイン*など）。必要なエントリを選択し、追加でボックスが表示される場合は、該当するすフィルタの条件を指定します。または、下部にあるドロップダウンリストを使用して、時刻によってエントリをフィルタリングできます。フィルタを適用するには、そのつど「*更新*」ボタンをクリックします。

デフォルトでは、1ページあたり20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。「*行数*」ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

表の列のヘッダをクリックすると、すべてのデータを並べ替えることができます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー（表示）から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

17.6.3 ブロックメール

「*Eメールプロテクション > ブロッメール*」タブには、アンチウイルスおよびアンチスパムによってブロックされたすべてのメール要求に関する包括的な統計が表示されます。

最初のドロップダウンリストから、表示するデータのタイプを選択します(例: *上位スパムブロック判定理由*や*上位ブロックマルウェア*など)。必要なエントリを選択し、追加でボックスが表示される場合は、該当するすフィルタの条件を指定します。または、下部にあるドロップダウンリストを使用して、時刻によってエントリをフィルタリングできます。フィルタを適用するには、そのつど「*更新*」ボタンをクリックします。

デフォルトでは、1ページあたり20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。「*行数*」ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

表の列のヘッダをクリックすると、すべてのデータを並べ替えることができます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

17.6.4 非匿名化

「*Eメールプロテクション > 非匿名化*」タブは、匿名化が有効になっている場合のみアクセス可能です(「*ログとレポート > レポーティング設定 > 匿名化*」を参照)。

ここでは、メールプロテクションレポートで特定のメールアドレスやドメインの匿名化を中止することができます。次の手順で実行します。

1. **両方のパスワードを入力します。**
   匿名化を有効にするために指定した1番目と2番目のパスワードを入力します。
2. **次の設定を行います。**
   アドレスの非匿名化:非匿名化するメールアドレスを追加します。

   非匿名化するドメイン:非匿名化するドメインを追加します。
3. **「*適用*」をクリックします。**
   設定が保存されます。

   指定したメールアドレスとドメインはレポートに表示されるようになります。

17.7 ワイヤレスプロテクション

「*ログとレポート > ワイヤレスプロテクション*」メニューのタブには、Sophos UTM によって検出された関連ワイヤレスプロテクションイベントについての統計の概要が表示されます。

17.7.1 デイリー

「*ワイヤレスプロテクション > デイリー*」タブは、ワイヤレスネットワークおよびアクセスポイントに関する過去 24時間の統計概観を示します。

SSID別レポーティング

各ワイヤレスネットワークのチャートが表示されます。各チャートには、次の 2つのグラフが表示されます。

- **接続クライアント:**ワイヤレスネットワークカードに接続しているクライアントの数。
- **失敗した接続試行回数:**ワイヤレスネットワークで接続に失敗した試行回数。

AP別レポーティング

各アクセスポイントについて、最大および平均の接続ユーザ数、アップタイム(過去 24時間でアクセスポイントが稼働していた累積時間)、および再接続の数がテーブルに表示されます。

17.7.2 ウィークリー

「*ワイヤレスプロテクション > ウィークリー*」タブには、過去 7日間のワイヤレスネットワークおよびアクセスポイントに関する概要的な統計が表示されます。ヒストグラムについては、「デイリー」のセクションを参照してください。

17.7.3 マンスリー

「*ワイヤレスプロテクション > マンスリー*」タブには、過去 4週間のワイヤレスネットワークおよびアクセスポイントに関する概要的な統計が表示されます。ヒストグラムについては、「デイリー」のセクションを参照してください。

17.7.4 年次

「*ワイヤレスプロテクション > 年次*」タブには、過去 12か月間のワイヤレスネットワークおよびアクセスポイントに関する概要的な統計が表示されます。ヒストグラムについては、「デイリー」のセクションを参照してください。

17.8 リモートアクセス

「*ログとレポート > リモートアクセス*」メニューのタブは、リモートアクセスアクティビティおよびセッション情報に関する全体的な統計を提供します。

17.8.1 アクティビティ

「*リモートアクセス > アクティビティ*」タブは、さまざまな期間について IPsec、SSL VPN、PPTP、および L2TP のUTMのリモートアクセスアクティビティに関する統計概要を提供します。

- デイリー
- ウィークリー
- マンスリー
- 年次

時間を選択:ドロップダウンリストを使用して、レポート期間を選択します。ページは自動的にリロード（再読み込み）されます。

17.8.2 セッション

「*リモートアクセス > セッション*」タブは、さまざまな時間範囲について、完了したセッション、失敗したログイン、および現在のユーザに関する包括的な統計を提供します。

注 – 「*Up*」および「*Down*」列にリモートアクセス接続のアカウンティングデータが表示されます。アカウンティングはシステムへの負荷を増やすため、デフォルトでは無効になっています。「*リモートアクセスアカウンティング*」セクションの「*レポート設定 > 設定*」タブで有効にできます。

最初のドロップダウンリストで、表示するセッションタイプを選択できます（*現在のユーザ*、*完了したセッション*、*失敗したログイン*）。フィルタを適用するには、「*更新*」ボタンをクリックします。

2番目のドロップダウンリストで結果をフィルタできます。選択したセッションタイプによっては、異なるフィルタが利用できます(例: *サービス別*または*送信元 IP アドレス別*)。一部のフィルタにはフィルタ引数を選択または入力する必要があります。

3番目のドロップダウンリストで結果を時間別にフィルタできます。フィルタを適用するには、その都度「*更新*」ボタンをクリックします。

デフォルトでは、1ページあたり 20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。「*行数*」ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

表の列のヘッダをクリックすると、すべてのデータを並べ替えることができます。

タブ右上隅の対応するアイコンをクリックすると、データを PDF あるいは Excel 形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

17.9 Web サーバプロテクション

「*ログとレポート > Web サーバプロテクション*」メニューのタブは、Web サーバの要求、警告、アラートに関する概要的な統計を表示します。

17.9.1 使用状況グラフ

「*Web サーバプロテクション > 使用状況グラフ*」タブは、さまざまな時間枠内にUTMで発生した Web サーバの要求、警告、アラートに関する概要的な統計を表示します。

- デイリー
- ウィークリー
- マンスリー
- 年次

17.9.2 詳細

「*Web サーバプロテクション > 詳細*」タブには、さまざまな時間枠内で最もアクティブだったクライアント、仮想ホスト、バックエンド、応答コード、および様々な攻撃に関する包括的な統計が表示されます。

最初のドロップダウンリストから、表示するデータのタイプを選択します(例: *上位クライアント*や*上位攻撃者*、*仮想ホスト別*など)。必要なエントリを選択し、追加でボックスが表示される場合は、該当するすフィルタの条件を指定します。または、下部にあるドロップダウンリストを使用して、時刻によってエントリをフィルタリングできます。フィルタを適用するには、そのつど「*更新*」ボタンをクリックします。

デフォルトでは、1ページあたり20件表示されます。それを超える数のエントリがある場合は、「次へ」/「戻る」アイコンを使用して前後のページに移動できます。「*行数*」ドロップダウンリストで、1ページに表示するエントリの数を変更できます。

タブ右上隅の対応するアイコンをクリックすると、データをPDFあるいはExcel形式でダウンロードできます。レポートは、現在選択されているビュー(表示)から生成されます。さらに、「円グラフ」アイコンが表示されている場合、それをクリックすると、表の上に円グラフが表示されます。

表の列のヘッダをクリックすると、すべてのデータを並べ替えることができます。

17.10 エグゼクティブレポート

「*ログとレポート > エグゼクティブレポート*」メニューでは、各サービスのネットワーク使用状況を表示するために重要なレポーティングデータをグラフィカルな形式にまとめることができます。

17.10.1 レポートを見る

「*ログとレポート > エグゼクティブレポート > レポートを見る*」タブでは、「*レポーティング*」メニューのタブとページにある個々のレポートに基づいて、完全なエグゼクティブレポートを作成することができます。エグゼクティブレポートを表示するウィンドウを開くには、「*レポートの作成*」ボタンをクリックします。

17.10.2 アーカイブエグゼクティブレポート

「*エグゼクティブレポート > アーカイブエグゼクティブレポート*」タブには、アーカイブされたすべてのエグゼクティブレポートの概要が表示されます。「*設定*」タブでアーカイブが選択されているエグゼクティブレポートのみがアーカイブされます。

17.10.3 設定

「*エグゼクティブレポート > 設定*」タブでは、エグゼクティブレポートの設定を行うことができます。

デイリーエグゼクティブレポート

デイリーエグゼクティブレポート:有効にすると、エグゼグティブレポートが毎日作成されます。

PDFレポートをアーカイブ:有効にすると、デイリーエグゼグティブレポートが PDF 形式でアーカイブ化されます。アーカイブ化されたエグゼクティブレポートには*アーカイブエグゼクティブレポート*からアクセスできます。

HTML ではなくPDF 形式でレポートを送信:有効にすると、メールエグゼグティブレポートが PDF ファイルとしてメールに添付して送信されます。有効にしない場合は、HTML 形式で送信されます。

メールアドレス:エグゼクティブレポートの受信者のメールアドレスを入力します。

ウィークリーエグゼクティブレポート

大部分の設定については、「*デイリーエグゼクティブレポート*」のセクションを参照してください。

このレポートでは、エグゼクティブレポートがデータの収集を開始する曜日も選択できます。

マンスリーエグゼクティブレポート

大部分の設定については、「*デイリーエグゼクティブレポート*」のセクションを参照してください。

17.11 ログ設定

「*ログとレポート > ログ設定*」メニューで、ローカルおよびリモートログの基本的な設定を構成できます。

17.11.1 ローカルログ

「*ログとレポート > ログ設定 > ローカルログ*」タブで、ローカルログの設定を行うことができます。デフォルトではローカルログは有効になっています。

ただし、ローカルログが無効になっている場合は、以下の手順で有効にできます。

1. **「*ローカルログ*」タブでローカルログを有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチが緑色に変わり、このタブ内のエリアが編集可能になります。

2. **いつログファイルを削除するか、期限を選択します。**
   ドロップダウンリストから、ログファイルに自動的に適用するアクションを選択します。デフォルトでは、「*ログファイルを削除しない*」が選択されています。

3. **「*適用*」をクリックします。**
   設定が保存されます。

しきい値

ここでローカルログのしきい値を定義できます。しきい値は、この値に達した場合に実行される特定のアクションに結び付けられます。次の作業を実行できます。

- **なし:**何も起こりません。
- **通知の送信:** :しきい値に達したことを管理者に伝える通知を送信します。
- **古いログから削除:**残りの量が設定したしきい値より下になるまで、あるいはログファイルのアーカイブが空になるまで、最も古いログファイルが削除されます。さらに、そのアクションの通知が管理者に送信されます。
- **システムのシャットダウン:**システムがシャットダウンします。そのイベントの通知が管理者に送信されます。
  システムをシャットダウンする場合は、管理者はローカルログの設定を変更し、ログファイルの削除を設定するか、あるいはログファイルを手動で移動/削除する必要があります。システムシャットダウンの理由が持続する場合は、次回のログ消去プロセスの実行時(毎日午前 12:00 つまり真夜中に実施)にシステムは再び自らをシャットダウンします。

設定を保存するには「*適用*」をクリックします。

17.11.2 Syslog送信ログ選択

「*ログとレポート > ログ設定 > リモート Syslog サーバ*」タブで、リモートログの設定を行うことができます。この機能により、UTMから他のホストにログメッセージを転送できます。これは、ホストを使用していくつかのUTMからログ情報を収集するネットワークに特に役立ちます。選択したホストでは、Syslog プロトコル互換のログデーモンを実行する必要があります。

リモート syslog サーバを設定するには、以下の手順に従います。

1. **「*リモート Syslog サーバ*」タブでリモート syslog を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*リモート Syslog 設定*」エリアが編集可能になります。

2. **「*Syslog サーバ*」ボックスの「+」アイコンをクリックしてサーバを作成します。**
「*Syslog サーバの追加*」ダイアログボックスが開きます。

3. **次の設定を行います。**
名前:リモート syslog サーバを説明する名前を入力します。

サーバ:UTMからログデータを受信する必要があるホストを追加または選択します。

警告 – UTM自体のインタフェースをリモート syslog ホストとして使用しないでください。これを行うと、ログループになります。

ポート:接続に使用するポートを追加または選択します。

4. **「*適用*」をクリックします。**
設定が保存されます。

リモート Syslog バッファ

このエリアで、リモート syslog のバッファサイズを変更できます。バッファサイズはバッファに保持されるログの行数です。デフォルトは 1000 です。設定を保存するには「*適用*」をクリックします。

リモート Syslog ログの選択

このエリアはリモート syslog が有効なときのみ編集できます。syslog サーバに送信するログのチェックボックスにチェックを入れてください。「*すべてを選択*」オプションを選択すると、一度にすべてのログを選択することができます。設定を保存するには「*適用*」をクリックします。

17.11.3 リモートログファイルアーカイブ

「*ログとレポート > ログ設定 > リモートログファイルアーカイブ*」タブで、ログファイルのリモートアーカイブを設定することができます。リモートログファイルのアーカイブを有効にすると、前日のログファイルは1つのファイルに集約・圧縮され、リモートログファイルのストレージに転送されます。ドロップダウンリストで転送方法を選択できます。

リモートログファイルのアーカイブを設定するには、以下の手順に従います。

1. ***リモートログファイルアーカイブ*機能を有効にします。**
トグルスイッチをクリックします。

トグルスイッチがアンバー色になり、「*リモートログファイルアーカイブ*」エリアが編集可能になります。

2. **ログファイルのアーカイブ方式を選択します。**
ドロップダウンリストで、希望のアーカイブ方式を選択します。選択した方式に応じて、各アーカイブ方式に関連する設定オプションが下に表示されます。以下のアーカイブ方式から選択できます。

- **FTP サーバ:***FTP (ファイル転送プロトコル)*方式では、以下のパラメータを設定する必要があります。
  - **ホスト:**FTP サーバのホストの定義。
  - **サービス:**サーバがリスンする TCP ポート。
  - **ユーザ名:**FTP サーバアカウントのユーザ名。
  - **パスワード:**FTP サーバアカウントのパスワード。
  - **パス:**ログファイルが保存されているリモート(相対)パス。
- **SMB (CIFS) 共有:**SMB 方式では、以下のパラメータを設定する必要があります。
  - **ホスト:**SMB サーバのホストの定義。
  - **ユーザ名:**SMB アカウントのユーザ名。
  - **パスワード:**SMBアカウントのパスワード。

    セキュリティに関する注記 – パスワードは設定ファイルにプレーンテキストで保存されます。したがって、このログに固有のユーザ/パスワードの組み合わせを作成することをお勧めします。

  - **共有:**SMB 共有名。ログファイルの転送先のパスまたはネットワーク共有情報を入力します(例: `/logs/log_file_archive`)。
  - **ワークグループ/ドメイン:**ログファイルのアーカイブを入れるワークグループまたはドメインを入力します。
- **Secure Copy (SSH サーバ):**SCP 方式を使用するには、公開 SSH DSA 鍵を、お使いの SCP サーバの承認済み鍵に追加する必要があります。Linux システムでは、SSH DSA 鍵をカットペーストして、設定されたユーザアカウントの `~/.ssh/authorized_keys` ファイルに追加できます。インスートール時にSophos UTMによって新しい SSHDSA 鍵が作成されます。セキュリティ上の理由から、この SSH DSA 鍵はバックアップには含まれません。したがって、新規またはバックアップのインストール後に、新しい SSH DSA 鍵をリモートサーバに保存して、ログファイルのアーカイブを SCP サーバに安全にコピーできるようにする必要があります。
  SCP 方式に以下の設定が必要です。

- **ホスト**:SCP サーバのホストの定義。
- **ユーザ名**:SCP サーバアカウントのユーザ名。
- **パス**:ログファイルの保存先の(完全な)リモートパス。
- **公開 DSA 鍵**:リモートストレージホスト上で、提供された公開 DSA 鍵を承認済み鍵のリストに追加します。

- **メールで送信**:ログファイルのアーカイブをメールで送信するために、有効なメールアドレスを入力します。

3. **「*適用*」をクリックします。**
   設定が保存されます。

転送が失敗すると、アーカイブはUTMに残ります。それぞれのログ削除プロセス時に、UTMは残りのすべてのアーカイブを配信しようと試みます。

17.12 レポート設定

「*ログとレポート > レポート設定*」メニューで、レポーティングの特定機能の有効化/無効化やデータ保持時間/量の設定といったレポーティング機能の設定を行うことができます。さらに、プライバシー保護を強化するためにデータを匿名にすることができます。

17.12.1 設定

「*設定*」タブで、レポートアクションおよびレポートデータが自動的に削除されるまでのシステムでの保持期間を定義できます。以下のレポートトピックを設定できます。

- アプリケーションコントロール
- 認証
- Eメールプロテクション
- ファイアウォール
- IPS
- ネットワーク使用状況
- リモートアクセス
- Web プロテクション
- Web サーバプロテクション

左側のチェックボックスを使用して、特定トピックに関するレポートを有効/無効にします。デフォルトでは、すべてのレポートトピックが有効になっています。

右側のドロップダウンリストを使用して、レポートデータの保持期間を設定します。

Note – 不要なレポートを無効にすることで、マシンの基本的な負荷を減らし、パフォーマンスのボトルネックを削減できます。レポートの保持期間はできるだけ短く設定してください。保存データの量が多いと基本的な負荷が高くなり、動的なレポートページの応答性を低下させます。

このタブの設定は、ログファイルアーカイブへは影響しません。

Webプロテクションレポート詳細レベル

このセクションでは、Web プロテクションレポートの詳細レベルを定義することができます。詳細レベルを高くすると、メモリの使用量とシステム負荷が目に見えて増加するため、必要でない限りは、詳細レベルを低くしてください。

以下の詳細レベルを設定できます。

- **ドメインのみ:**レポートには、URL のトップレベルドメインとセカンドレベルドメイン(例: `example.com`)が表示されます。サードレベルドメインは、強制すると表示されます(例: `example.co.uk`)。
- **フルドメイン:**レポートには、フルドメインが表示されます(例: `www.example.com`、`shop.example.com`)。
- **1レベルのURL:**レポートには、URLの最初の(仮想)ディレクトリが追加で表示されます(例: `www.example.com/en/`)。
- **2レベルのURL:**レポートには、URL の最初の 2つの(仮想)ディレクトリが追加で表示されます(例: `www.example.com/en/products/`)。
- **3レベルのURL:**レポートには、URL の最初の 3つの(仮想)ディレクトリが追加で表示されます(例: `www.example.com/en/products/new/`)。

エグゼクティブレポート設定

このエリアで、保持するエグゼクティブレポートの数をそれぞれ定義できます。

- デイリーレポート:最大 60
- ウィークリーレポート:最大 52
- マンスリーレポート:最大 12

設定を保存するには「*適用*」をクリックします。

エグゼクティブレポートとそのオプションに関する詳細は、「*ログとレポート > エグゼクティブレポート*」を参照してください。

PDF 用紙設定

PDF エグゼクティブレポートのデフォルトの用紙サイズは A4 です。ドロップダウンリストを使用して、「*レター*」または「*リーガル*」を選択できます。設定を保存するには「*適用*」をクリックします。

リモートアクセスアカウンティング

リモートアクセス接続のアカウンティングを有効または無効にできます。有効にすると、リモートアクセス接続に関するデータが保管され、「*ログとレポート > リモートアクセス > セッション*」タブの「*Down*」および「*Up*」列に表示されます。無効にすると、アカウンティングは停止します。この機能を有効にすると、システムへの負荷が増大する可能性があります。

CSV 区切り文字設定

ここでは、CSV 形式へのレポーティングデータのエクスポート時に使用するデリミタを定義できます。Windows オペレーティングシステムでは、エクスポートするデータが Excel などの表計算プログラムで正確に表示されるようにするために、デリミタがシステムの地域設定と一致する必要があります。

IPFIX アカウンティング

IPFIX を使用して、UTMの IPv4 フローデータをプロバイダにエクスポートし、モニタリング、レポート、アカウンティング、料金請求などのために使用することができます。

IPFIX (Internet Protocol Flow Information Export) は、アカウンティング情報を普遍的な方法でエクスポートするためのメッセージベースのプロトコルです。アカウンティング情報は、*エクスポータ*により収集され、*コレクタ*に送信されます。IPv4 フローの一般的なアカウント情報は、*送信元アドレス*、*宛先アドレス*、*送信元ポート*、*宛先ポート*、*バイト*、*パケット*、*およびネットワークトラフィック分類データ*で構成されます。

有効にすると、UTM はエクスポータとして機能します。IPFIX アカウンティング情報をエクスポートします。コレクタは通常プロバイダのサイトに配置され、ここで 1つ以上のUTMのアカウンティングデータが集約されて分析されます。プロバイダでのシステムのセットアップ時にホスト名が提供され、1つのエクスポータ、つまりUTM毎に一意の OID (Observation Domain ID) を定義する必要があります。このデータを該当するフィールドに入力します。

データは、UDP ポート 4739 でエクスポートされます。1つのネットワーク接続が、エクスポート方向のために1つと応答のために 1つの合計 2つの IPFIX フローを使用します。

注セキュリティ – IPFIX のアカウントデータは暗号化のない状態で送信されることに注意して下さい。ゆえにこのデータの送信はプライベートネットワーク経由で行われることを推奨します。

設定を保存するには「*適用*」をクリックします。

17.12.2 除外

「*レポート設定 > 除外*」タブで、特定のドメインやアドレスをレポートから除外できます。これはエグゼクティブレポートに加え、「*ログとレポート*」ページと統計概要ページに影響を及ぼします。

注 – 今日の統計ページの情報は、10～15分毎に更新されるのみであるため、この影響が統計ページに直ちに表れるわけではありません。インポート機能によって複数の項目を一度に定義することも可能です。

レポーティング除外:Web

このセクションには、すべてのWebプロテクションレポートから除外するドメインを定義できます。ドメイン名には、「*ログとレポート > Web プロテクション > Web 使用状況レポート*」タブの「*ドメイン*」レポートにリストされたものとまったく同じ名前を指定する必要があります。設定を保存するには「*適用*」をクリックします。

レポーティング除外:メール

これらの 2つのセクションには、すべてのメールプロテクションレポートから除外するドメインとメールアドレスを定義できます。

特定のドメインのすべてのメールアドレスを除外するには、「*ドメイン*」ボックスを使用します。`sophos.com` のように、メールアドレスのドメイン部分のみを入力します。レポートから特定のメールアドレスを除外するには、「*アドレス*」ボックスを使用します。設定を保存するには「*適用*」をクリックします。

指定したドメイン名またはアドレスを含む送信者または受信者のメールが、すべてのメールプロテクションレポートから除外されます。

レポーティング除外:ネットワークプロテクション

このセクションには、すべてのネットワークプロテクションレポートから除外するIPv4 および IPv6 アドレスを定義できます。設定を保存するには「*適用*」をクリックします。

レポーティング除外:ネットワークアカウンティング

このセクションには、すべてのネットワーク使用状況レポートから除外するIPv4およびIPv6アドレスを定義できます。設定を保存するには「*適用*」をクリックします。

17.12.3 匿名化

「*レポート設定 > 匿名化*」タブでは、「4つの目の原則」(four-eyes principle)に基づいてデータを匿名にできます。これは、2人の人間がその手順を承認した場合のみ非匿名化できることを意味します。匿名にすると、ユーザデータのレポートを表示する際にそのデータの機密性が保たれるため、アクション(Webサーフィンなど)から特定の人間にトレースバックする(さかのぼる)ことができなくなります。

匿名にするには、以下の手順に従います。

1. **「*匿名化*」タブで匿名化を有効にします。**
   トグルスイッチをクリックします。

   トグルスイッチがアンバー色になり、「*匿名化設定*」エリアが編集可能になります。

2. **2つのセキュリティパスワードを入力します。**
   「4つの目の原則」は、異なる2人の人間が互いが秘匿しているパスワードを入力したときのみ有効です。

3. **「*適用*」をクリックします。**
   設定が保存されます。

匿名化を再度グローバルに無効にするには、その両方のパスワードが必要になります。

1. **「*匿名化*」タブで、トグルスイッチをクリックします。**
   トグルスイッチがアンバー色になり、「*匿名化設定*」エリアが編集可能になります。

2. **両方のパスワードを入力します。**
   匿名化を有効にするために指定した1番目と2番目のパスワードを入力します。

3. **「*適用*」をクリックします。**
   設定が保存されます。

必要に応じて、匿名化を1人のユーザに対して無効にできます。詳細は「*ログとレポート >> Webプロテクション*」および「*ログとレポート > Eメールプロテクション*」を参照してください。

18 サポート

この章では、Sophos UTMで使用できるサポートツールについて説明します。

「*サポート*」メニューのページには、さまざまなWebリンク、お問い合わせ情報、役立つネットワークツールの出力など、お客様サポート関連の多数の機能が含まれています。これらを活用されることで、UTMのコマンドラインインタフェースを使用しないで、重要なネットワークプロパティを判断することができます。

この章では、次のトピックについて説明します。

- ドキュメント
- 印刷可能形式設定情報
- サポート窓口
- ツール
- 詳細

さらに、「*サポート*」メニューのメインページには、以下の情報へのWebリンクが含まれています。

- **サポートデータベース**(KB):Sophos NSGの公式サポートデータベースには、Sophos UTMの設定に関するさまざまな情報が掲載されています。
- **既存の問題点リスト**(KIL):解決できない既知の問題や対応策のある既知の問題のリストです。
- **ハードウェア互換性リスト**(HCL):Sophos UTMソフトウェアに対応するハードウェアのリストです。
- **Up2Date情報**:Sophos NSGUp2Dateブログには、製品の改善やファームウェアの更新についての情報が掲載されています。

18.1 ドキュメント

オンラインヘルプ

このセクションには、オンラインヘルプの開き方、および使用に関する説明があります。

マニュアルのダウンロード

最新の管理ガイドをPDF 形式でダウンロードできます。ガイドの言語を選択し、「*ダウンロード開始*」をクリックします。PDF 文書を開くためには、Adobe Reader や Xpdf といった専用のリーダーが必要です。

参照 – 旧バージョンの UTM の管理ガイドや、その他のドキュメントは、Sophosサポートデータベースよりダウンロードできます。

18.2 印刷可能形式設定情報

「*サポート > 印刷可能形式設定情報*」ページでは、現在の WebAdmin 設定について詳細なレポートを作成できます。

注 – 印刷可能形式設定情報は新しいウィンドウで開きます。ブラウザによっては、WebAdmin 用にポップアップウインドウを許可する必要があります。

印刷可能形式設定情報の構造は、WebAdmin メニューの構造と同じであるため、対応する WebAdmin の設定オプションを簡単に見つけることができます。

印刷可能形式設定情報ブラウザページは、概要ページ（*索引*）と複数のサブページから成ります。サブページへのリンクはブルーでハイライトされています。サブページには、関連トピックの詳細情報が表示されます。サブページの下部にある「*索引に戻る*」リンクをクリックして、いつでもサブページから索引に戻ることができます。

印刷可能形式設定情報には他に2つの表示オプションがあります。

- WebAdmin 形式
- Confd 形式

これらの表示オプションへのリンクは、索引ページの下部にあります。

18.3 サポート窓口

Sophos は、セキュリティソリューションのために総合的なカスタマーサポートサービスを提供しています。お客様の サポート/メンテナンスレベルに応じて、さまざまなレベルのアクセスサービスに加

え、Sophos サービス部門や Sophos NSG 認定パートナーによるさまざまなレベルのサポートを提供しています。

Sophos UTM に関連するすべてのサポートケースは、MyAstaro ライセンスポータル経由で処理されます。サポートケースを開くには、「*新しいウィンドウでサポートチケットをオープンする*」をクリックして Web フォームを使用してください。

18.4 ツール

「*サポート > ツール*」メニューのタブには、有用なネットワークツールの出力が表示されます。これらを使用すると、UTM のコマンドラインインタフェースを使用しないで、重要なネットワークプロパティを判断することができます。ここでは、以下のツールの出力を見ることができます。

- Ping
- Traceroute
- DNS ルックアップ

18.4.1 Ping チェック

ping プログラムは、IP ネットワークを横断して特定ホストに到達できるかどうかをテストするためのコンピュータネットワークツールです。ping は、ICMP *エコー要求*パケットをターゲットホストに送信し、ICMP *エコー応答*による返信を待機することで機能します。ping は、間隔のタイミングと応答率を使用して、ホスト間の往復時間とパケット紛失率を評価します。

ping チェックを行うには、以下の手順に従います。

1. **ping ホストを選択します。**
   ping するホストを選択します。「*Ping ホスト*」ボックスで、ホスト定義のあるホストを選択できます。または、「*ホスト名/IP アドレスを入力*」を選択してカスタムホスト名または IP アドレスを下のテキストボックスに入力することもできます。
2. **IP バージョンを選択します**(IPv6 をグローバルに有効にしている場合にのみ使用可能です)。
   「*IP バージョン*」ドロップダウンリストで、「*IPv4*」または「*IPv6*」を選択します。
3. **「*適用*」をクリックします。**
   ping チェックの出力が「*Ping チェック結果*」エリアに表示されます。

18.4.2 Traceroute

traceroute(トレースルート)プログラムは、IP ネットワーク上でパケットが使用するルートの決定に使用されるコンピュータネットワークツールです。traceroute は、パケットの伝送に関与したルータの IP アドレスを一覧表示します。一定の時間内にパケットのルートを判断できない場合は、IP アドレスの代わりにアスタリスク(*)で報告します。一定の回数だけ失敗すると、確認作業は終了します。確認の中断には多くの理由が考えられますが、ほとんどの場合は、ネットワークパスのファイアウォールが traceroute パケットをブロックすることが原因となります。

ルートを追跡するには、以下の手順に従います。

1. **traceroute ホストを指定します。**
   ルートを追跡するホストを指定します。「*Traceroute 先ホスト*」ボックスで、ホスト定義のあるホストを選択できます。または、「*ホスト名/IP アドレスを入力*」を選択してカスタムホスト名または IP アドレスを下のテキストボックスに入力することもできます。
2. **IP バージョンを選択します**(IPv6 をグローバルに有効にしている場合にのみ使用可能です)。
   「*IP バージョン*」ドロップダウンリストで、「*IPv4*」または「*IPv6*」を選択します。
3. **ホップアドレスをホスト名解決せず、数字で表示**(任意)。
   パスで見つかった各ゲートウェイについて、ネームサーバで IP アドレスから DNS ホスト名への名前解決を行わない場合は、このオプションを選択します。
4. **「*適用*」をクリックします。**
   traceroute の出力が「*トレースルートの結果*」エリアに表示されます。

18.4.3 DNS ルックアップ

dig プログラム(*Domain Information Groper* の略)は、DNS ネームサーバに問い合わせを行うネットワークツールです。dig プログラムは DNS ルックアップを実行し、クエリしたネームサーバから返された応答を表示します。

DNS ルックアップを行うには、以下の手順に従います。

1. **ホスト名/IP アドレスを指定します。**
   DNS 情報を判定したいホストのホスト名または IP アドレスを入力します。
2. **「*詳細出力の有効化*」を選択します**(任意)。
   このオプションを選択すると、より詳細な情報が出力されます。

3. **「*適用*」をクリックします。**
   dig の出力が「*DNS ルックアップの結果*」エリアに表示されます。

18.5 詳細

「*サポート > 詳細*」メニューには、UTM に関するより詳細な情報が表示され、高度な機能が提供されています。ここには、実行中のプロセスとローカルネットワーク接続の概要が表示され、ルーティングテーブルとインタフェーステーブルを確認することができます。さらに、デバッグやリカバリのためのサポートパッケージをダウンロードしたり、ログファイルに表示される内部使用の設定リファレンスに関する背景情報を確認することができます。

18.5.1 プロセスリスト

ps プログラムは、ヘッダ行に続き、コントロール端末を持つプロセスに関する情報を表示します。この情報は、コントロール端末毎にソートされ、次にプロセス ID 毎にソートされます。

18.5.2 LAN コネクション

コマンド *netstat*（「*ネットワーク統計*」の略語）とは、コンピュータに現在存在するアクティブなインターネット接続（受信と送信の両方）のリストを表示するネットワークツールです。

18.5.3 ルーティングテーブル

ip コマンドは、TCP/IP ネットワークのコントロールとトラフィックコントロールのためのネットワークツールです。パラメータ `route show table all` 付きで実行されるこのコマンドは、UTM のすべてのルーティングテーブルの内容を表示します。

18.5.4 インタフェーステーブル

このテーブルには、Sophos UTMのすべての設定済みインタフェース（ネットワークインタフェースカードと仮想インタフェースの両方）が表示されます。`addr` パラメータ付きで実行した *ip* コマンドが、インタフェースとそのプロパティを表示します。

18.5.5 コンフィグダンプ

デバッグやリカバリのために、Sophos UTMのインストールに関してできるだけ多くの情報を収集しておくと便利です。これには、「*サポート > 詳細 > コンフィグダンプ*」タブでダウンロード可能なサポートパッケージを使用できます。`zip` ファイルには次のアイテムが含まれています。

- UTM 設定の全ダンプ(`storage.abf`)。これは真のバックアップファイルではないため、パスワードなどが含まれておらず、デバッグ目的のみで使用できます。
- システム内に存在するハードウェアに関する情報(`hwinfo`)。
- システムにインストールされたソフトウェアパッケージに関する情報(`swinfo`)。

18.5.6 REF_ をリゾルブ

デバッグのために、システム内部で使用されている設定リファレンスをリゾルブすることができます。ログ内でリファレンスを見つけた場合、リファレンス文字列をここに貼り付けてください(例: `REF_DefaultSuperAdmin`)。タブに、設定用 Configuration デーモンのデータ構造の該当箇所が表示されます。

19 ログオフ

UTM からログアウトするには、「*ログオフ*」メニューエントリをクリックします。適切にログアウトしなかった場合や、Webブラウザを誤って閉じてしまった場合には、約30秒間再ログインできない可能性があります。

注 – セッション中に別のWebサイトにアクセスした場合にも、ログアウトしたことになります。この場合、ログインしなおす必要があります。

20 ユーザポータル

ここでは、ユーザポータルの機能およびここでエンドユーザに提供されるサービスについて説明します。

Sophos UTMのユーザポータルは、許可したユーザにパーソナルなメールおよびリモートアクセスを中心としたサービスを提供するブラウザベースアプリケーションです。ユーザポータルにアクセスするには、Sophos UTMの URL（`https://192.168.2.100` など）にブラウズします（HTTPS プロトコル）。

ログインページで、ユーザはヘッダバーの右側にあるドロップダウンリストから言語を選択できます。

管理者が WebAdmin で有効にしたサービスおよび機能に応じて、ユーザは以下のサービスにアクセスできます。

- メール隔離
- メールログ
- POP3 アカウント
- 送信者ホワイトリスト
- 送信者ブラックリスト
- ホットスポット
- クライアント認証
- リモートアクセス
- HTML5 VPN ポータル
- パスワードの変更
- HTTPS プロキシ

20.1 ユーザポータル:隔離メール

メール隔離機能により、ユーザは隔離されているメッセージを表示したり、リリースすることができます。

注 –「*メール隔離*」タブは、ユーザのメールアドレスがによりモニタリングされるネットワークまたはドメインに属し、管理者によってユーザにこの機能のアクセス権が割り当てられている場合にのみ表示されます。ユーザが SMTP と POP3 の両方でメールを受信する場合は、メールが「*POP3 隔離*」および「*SMTP 隔離*」の 2つのタブに編成されます。これらのタブの機能は同じです。

「*メール隔離*」タブには、ユーザ宛てに送信され、Sophos UTMによってブロックおよび隔離されたすべてのメールの概要が表示されます。POP3 の隔離メールが表示されるようにするには、ユーザは「*POP3 アカウント*」タブにユーザの POP3 資格情報を入力する必要があります。

隔離メールのソートとフィルタ

デフォルトではすべてのメールが表示されます。リストに 20件を超えるメールが含まれる場合、複数ページに分割され、「>」(次へ)ボタンと「<」(戻る)ボタンを使用して移動することができます。

表示オプションを変更するには、次の手順に従います。

Sort by(ソート順):デフォルトでは、受信時刻によりリストがソートされています。ここでは、別のソート基準を選択できます。

and show(表示):チェックボックスを選択することで、1ページあたり 20件、50件、100件、250件、500件、1000件、またはすべてのメッセージを表示することができます。すべてのメッセージの表示には時間がかかる場合があります。

以下の項目でメールをフィルタすることができます。

- **#隔離メッセージ:**ページ上部のチェックボックスを選択して、隔離理由(悪質なコンテンツ、スパム、表現との一致、ファイル拡張子、MIME タイプ、スキャン不可能など)別にメールを表示または非表示にできます。
- **アドレス:**送信者アドレスに応じてメッセージをフィルタできます。
- **送信者/件名 サブストリング:**送信者または件名を入力して、隔離されたメッセージを検索できます。
- **受信日:**特定の期間内に処理されたメッセージのみを表示するには、日付を入力するか、カレンダーアイコンで日付を選択します。

隔離メールの管理

それぞれのメッセージの前のチェックボックスを利用するか、メッセージをクリックし選択することにより、次の作業を実行できます。次の作業を実行できます。

- **表示:**メールのコンテンツを示すウィンドウを開きます。
- **ダウンロード:**選択したメッセージが EML 形式でダウンロードされます。
- **削除:**選択されたメッセージを削除します。これを取り消すことはできません。
- **送信者のホワイトリスト化:**メールを受信トレイに移動し、送信者をホワイトリストに追加します。今後この送信者から送られるメールが隔離されないようになります。悪質なコンテンツを含むメールは、ホワイトリストの送信者から送られている場合でも、常に隔離されます。
- **リリース:**選択されたメッセージを隔離からリリースします。

注 – ここで許可されるアクションは、メールが隔離された理由および WebAdmin の設定に基づいて異なります。ユーザは明示的に許可されているメッセージのみをリリースできます。隔離に保留されているメッセージをすべてリリースできるのは管理者だけです。

グローバルクリーンアップアクションの選択:ここには、メッセージに対してグローバルに適用されるさまざまな削除オプションがあります。つまり、選択されていないメッセージや表示されていないメッセージにもオプションが適用されます。

20.2 ユーザポータル:メールログ

このタブで、エンドユーザは SMTP 経由で送信されたメールのトラフィックのログを表示することができます。

注 –「*メールログ*」タブは、ユーザのメールアドレスが Sophos UTM の SMTP プロキシによりモニタリングされるドメインに属し、管理者によってユーザにこの機能のアクセス権が割り当てられている場合にのみ表示されます。ユーザが SMTP と POP3 の両方でメールを受信する場合、このタブの名前は「*SMTP ログ*」になります。

「*メールログ*」タブには、ユーザのメールアドレスのすべてのメールトラフィックに関するログエントリが示されます。未配信のメールのログエントリには、配信されなかった理由に関する情報が含まれます。ログエントリをダブルクリックすると、ウィンドウが開き、詳細なログ情報が表示されます。

デフォルトではすべてのメールが表示されます。リストに 20件を超えるメールが含まれる場合、複数ページに分割され、「>」(次へ)ボタンと「<」(戻る)ボタンを使用して移動することができます。

表示オプションを変更するには、次の手順に従います。

Sort by(ソート順):デフォルトでは、受信時刻によりリストがソートされています。ここでは、別

のソート基準を選択できます。

and show(表示):チェックボックスを選択することで、1ページあたり 20件、50件、100件、250件、500件、1000件、またはすべてのメッセージを表示することができます。すべてのメッセージの表示には時間がかかる場合があります。

以下の項目でメールをフィルタすることができます。

- **#ファイルのログイベント:**ページ上部のチェックボックスを選択して、ステータスに応じてメールを表示または非表示にできます。
- **アドレス:**送信者アドレスに応じてメールをフィルタできます。
- **送信者/件名 サブ文字列:**送信者または件名を入力して、隔離されたメッセージを検索できます。
- **受信日:**特定の期間内に処理されたメッセージのみを表示するには、日付を入力するか、カレンダーアイコンで日付を選択します。

20.3 ユーザポータル:POP3 アカウント

このタブで、エンドユーザは、自分宛ての POP3 隔離メールを表示・配信し、隔離リポートを受信するように設定できます。

注 – *POP3 アカウント* タブは管理者が POP3 を有効化し、POP3 サーバを追加した場合のみ利用できます。

このページで、ユーザは、使用する POP3 アカウントのアカウント情報を入力する必要があります。POP3 アカウント情報が入力されたスパムメールのみがユーザポータルに表示されます。POP3 アカウントのアカウント情報が保存されているユーザは、各メールアドレスについて、別々の隔離レポートを受け取ります。

20.4 ユーザポータル:送信者ホワイトリスト

送信者ホワイトリスト機能により、ユーザはメール送信者をホワイトリストに追加して、その送信者からのメッセージがスパムとして処理されないようにすることができます。ただし、ウイルスを含むメールやスキャン不可能なメールは隔離されます。

注 –「*送信者ホワイトリスト*」タブは、ユーザのメールアドレスがSophos UTMによりモニタリングされるネットワークまたはドメインに属し、管理者によってユーザにこの機能のアクセス権が割り当てられている場合にのみ表示されます。

ホワイトリストに送信者を追加するには、「+」アイコンをクリックしてアドレスを入力し、チェックアイコンをクリックして保存します。有効なメールアドレスを入力するか(`jdoe@example.com`など)、アスタリスクをワイルドカードとして使用して特定ドメインのすべてのメールアドレスを指定できます(`*@example.com`など)。

20.5 ユーザポータル:送信者ブラックリスト

このタブで、エンドユーザはメール送信者をブラックリストに追加して、その送信者からのメッセージを常にスパムとして処理することができます。

注 –「*送信者ブラックリスト*」タブは、ユーザのメールアドレスがSophos UTMによりモニタリングされるネットワークまたはドメインに属し、管理者によってユーザにこの機能のアクセス権が割り当てられている場合にのみ表示されます。

ブラックリストは、システム内でSMTPとPOP3が使用されていれば、SMTPとPOP3の両方のメールに適用されます。ブラックリストに送信者を追加するには、「+」アイコンをクリックしてアドレスを入力し、チェックアイコンをクリックして保存します。有効なメールアドレス(`phishing@hotmail.com`など)を入力するか、ドメイン全体(`*@hotmail.com`など)を指定することができます。

20.6 ユーザポータル:ホットスポット

ホットスポット機能により、カフェ、ホテル、企業などではゲストに時間制限やトラフィック制限を課したインターネットアクセスを提供できます。

注 – ユーザポータルの「*ホットスポット*」タブは、管理者がパスワードかバウチャータイプのホットスポットを作成し、ユーザを許可ユーザに追加している場合にのみ表示されます。

このタブでは、ワイヤレスネットワークのゲストにホットスポットアクセス情報を配信できます。タブで可能な機能は、選択したホットスポットのタイプに応じて、一般的なパスワードを配信するか、バウチャーを作成して配信するかのいずれかになります。

ホットスポットタイプ:当日有効パスワード

「*パスワード*」フィールドには、現在のパスワードが表示されます。パスワードは1日に1回自動的に変更されます。しかし、手動でパスワードを変更することができます。パスワードを変更すると、古いパスワードが即時に無効になり、アクティブなセッションが終了します。

パスワードを変更するには、次の手順に従います。

1. **ユーザポータルで、「*ホットスポット*」タブを選択します。**
2. **アクセス情報を管理するホットスポットを選択します。**
   「*ホットスポット*」ドロップダウンリストから、パスワードを変更するホットスポットを選択します。
3. **新しいパスワードを定義します。**
   「*パスワード*」フィールドに新しいパスワードを入力するか、「*生成*」ボタンをクリックして自動的に新しいパスワードを作成します。
4. **新しいパスワードをメールで送信するには、「*メール送信*」チェックボックスにチェックを入れます。**
   管理者によって指定されているメール受信者にパスワードが送信されます。管理者がメールアドレスを設定していない場合は、チェックボックスは選択できません。
5. **「*保存*」をクリックします。**
   パスワードが即時に変更されます。

ホットスポットタイプ:バウチャー

それぞれ一意のコードを持つバウチャーを作成することができます。バウチャーは印刷してゲストに提供することができます。作成したバウチャーのリストにより、バウチャーの使用状況を把握および管理できます。

バウチャーを作成するには、次の手順に従います。

1. **ユーザポータルで、「*ホットスポット*」タブを選択します。**
2. **アクセス情報を管理するホットスポットを選択します。**
   「*ホットスポット*」ドロップダウンリストから、バウチャーを作成するホットスポットを選択します。

3. **「バウチャー定義」フィールドからバウチャータイプを選択します。**
   バウチャータイプは管理者によって定義されています。どの目的にどのタイプのバウチャーを使用するかは、社内で定義する必要があります。
4. **「数」フィールドには、このタイプのバウチャーの作成数を入力します。**
5. **オプションで、「コメント」フィールドにコメントを入力します。**
   このコメントはバウチャーリストに表示されます。
6. **バウチャーを直接印刷するには、「印刷」チェックボックスにチェックを入れます。**
7. **「バウチャーの作成」ボタンをクリックします。**
   バウチャーが生成されます。下のバウチャーリストの新しい行に、各バウチャーが即時に表示されます。印刷を指定した場合は、バウチャーが直接印刷されます。各バウチャーには、一意のコードがあります。

注 – バウチャーの内容、サイズ、レイアウトは管理者によって設定されます。

バウチャーリストでバウチャーを管理することができます。リストの並べ替えやフィルタ、コメントの入力または変更、選択したバウチャーの印刷、削除、エクスポートを行うことができます。

- リストを並べ替えるには、「*ソート基準*」ドロップダウンリストから目的のソート基準を選択します。右のドロップダウンリストを使用すると、1ページに表示するバウチャーの数を変更できます。
- リストをフィルタするには、「*ステータス*」、「*コード*」、または「*コメント*」のいずれかのフィールドを使用します。入力するにつれ、リストが直接フィルタされます。フィルタをリセットするには、ステータスエントリの「すべて」を選択し、「*コード*」や「*コメント*」テキストフィールドからすべてのテキストを削除します。
- コメントを入力するか変更する場合は、各バウチャーの「*コメント*」列にあるメモ帳アイコンをクリックします。編集フィールドが表示されます。テキストを入力するか編集して Enter キーを押すか、チェックマークをクリックします。
- バウチャーを印刷するか削除するには、目的のバウチャーの前にあるチェックボックスにチェックを入れ、下部にある必要なボタンをクリックします。

  注 – バウチャーは、一定の時間の経過後に自動的に削除することができます。この時間は管理者が設定できます。

- バウチャーをエクスポートするには、次の手順に従います。目的のバウチャーの前にあるチェックボックスにチェックを入れ、下部にある「*CSV へのエクスポート*」ボタンをクリックします。ウィンドウが表示され、CSV ファイルを保存するか、CSV ファイルを直接開くかを選択で

きます。選択したバウチャーが 1つの CSV ファイルに保存されます。ファイルを開く際には、列の区切り文字として正しい文字を選択するようにしてください。

20.7 ユーザポータル:クライアント認証

クライアント認証を使用すると、ユーザはSophos Authentication Agent (SAA) のセットアップファイルをダウンロードできます。SAA は Web フィルタの認証モードとして使用できます。

注 –「*クライアント認証*」タブは、管理者によってクライアント認証が有効化されている場合にのみ使用できます。

20.8 ユーザポータル:リモートアクセス

リモートアクセス機能により、ユーザは提供されているリモートアクセスクライアントソフトウェアと設定ファイルをダウンロードすることができます。

注 –「*リモートアクセス*」タブは、ユーザに対して最低 1つのリモートアクセスモードが有効になっている場合のみ利用できます。

このページには、管理者がユーザに対して有効にしている接続タイプに対応するリモートアクセスデータのみが提供されます。たとえば、SSLVPN リモートアクセスのみが有効にされている場合、「*SSL VPN*」セクションのみが表示されます。

各接続タイプが別のセクションに表示されます。接続タイプによっては、各ソフトウェアをダウンロードするための情報やボタンがあります。該当する場合は、セクションの上部に「*新しいウィンドウでインストール手順を開く*」リンクが表示されます。これをクリックすると、詳細なインストール手順が開きます。

20.9 ユーザポータル:HTML5 VPNポータル

HTML5 VPN ポータルを使用すると、外部ネットワークのユーザは、ブラウザのみをクライアントとして使用して、あらかじめ設定されているコネクションタイプで内部リソースにアクセスすることができます。

注 –「*HTML5 VPN ポータル*」タブは、管理者が VPN コネクションを作成し、ユーザを許可ユーザに追加している場合にのみ表示されます。

注 – ブラウザは HTML5 に準拠したものである必要があります。HTML5 VPN 機能に対応しているブラウザは次のとおりです。Firefox 6.0 以降、Internet Explorer 10 以降、Chrome、Safari 5 以降(Mac 環境のみ)。

「*HTML5 VPN ポータル*」タブには、許可されているコネクションのリストが表示されます。アイコンにより、コネクションタイプが示されます。

コネクションを使用するには、次の手順に従います。

1. **それぞれの「*接続*」ボタンをクリックします。**
   新しいブラウザウィンドウが開きます。その内容とレイアウトはコネクションタイプに依存します。たとえば、HTTP または HTTPS コネクションを開いた場合には、Web サイトが含まれますが、SSH コネクションの場合はコマンドラインインタフェースとなります。
2. **新しい VPN ウィンドウで作業する。**
   一部のタスクでは、VPN ウィンドウの上部にカーソルを運ぶと、コネクションタイプ固有のメニューバーが表示されます。
   - **ファンクションキーやキーの組み合わせを使用する:**ファンクションキーや CTRL-ALT-DEL キーなどの特殊コマンドを使用する場合は、「*キーボード*」メニューの該当するエントリを選択する必要があります。
   - **ローカルホストから VPN ウィンドウへコピー & ペーストする:**ローカルコンピュータで、該当するテキストをクリップボードへコピーする必要があります。コネクションウィンドウで、「*クリップボード*」メニューを選択します。CTRL-V キーを押して、テキストをテキストボックスへ貼り付けます。次に「*サーバへ送信*」ボタンをクリックします。SSH や Telnet コネクションでは、テキストは直接カーソルの位置に貼り付けられます。RDP や VNC コネクションでは、テキストはサーバのクリップボードに送信された後、通常どおり貼り付けることができます。

     注 – コピー & ペーストは Webapp コネクションでは使用できません。

   - **VPN ウィンドウから別のウィンドウへコピー & ペーストする:**SSH および Telnet コネクションでは、ローカルウィンドウで実施する要領で、単純にテキストをコピーして貼り付けるだけです。RDP や VNC コネクションでは、VPN ウィンドウで、該当するテキストをクリップボードへコピーする必要があります。続いて「*クリップボード*」メニューを選択

します。コピーしたテキストがテキストボックスに表示されます。テキストを選択し、CTRL-C キーを押します。これでテキストがローカルのクリップボードに入り、通常どおり貼り付けることができます。

- **リモートデスクトップ接続でキーボードの配置を変更する:**Windows ホストを使用したリモートデスクトップ接続では、VPN ウィンドウのキーボード言語の設定を変更できます。特に Windows ログインの場合は、パスワードを正確にタイプしていることを確認するために、選択言語が Windows の言語設定と一致する必要があります。「*キーボード>キーボードレイアウト*」メニューで適切な言語を選択します。選択したキーボードレイアウトは cookie に保存されます。
- **Webapp コネクションでスタートページに戻る:**Webapp コネクションでデフォルトのページに戻るには、「*ナビゲーション>ホーム*」メニューを選択します。

3. **作業を完了したら、コネクションを閉じます。**
   - 最終的に接続を終了するには、「*接続*」メニューから「*セッションの停止*」コマンドを選択するか、タイトルバーの X アイコンをクリックしてブラウザウィンドウを閉じます。「*コネクション*」ボタンを再度使用して新規セッションを開始できます。
   - セッションを切断するには、「*コネクション*」メニューから「*セッションの停止*」コマンドを選択します。セッションのステータスは 5分間にわたって保存されます。この時間内に再接続すると、以前のセッションを継続できます。

20.10 ユーザポータル:パスワードの変更

パスワードの変更機能により、ユーザはユーザポータルにアクセスするためのパスワードと、使用できる場合は、PPTP を介したリモートアクセス用のパスワードを変更できます。

20.11 ユーザポータル:HTTPS プロキシ

HTTPS プロキシ機能により、ユーザは HTTP/S プロキシの CA 証明書をインポートして、セキュア Web サイトの訪問時に表示されるエラーメッセージを回避することができます。

注 – ユーザポータルの「*HTTPS プロキシ*」タブは、管理者によって HTTP/S プロキシの証明書が提供されているユーザのみに表示されます。

「*プロキシ CA 証明書をインポート*」をクリックすると、ユーザのブラウザに、他の目的に対して CA を信頼するかを確認するプロンプトが表示されます。

用語集

3

3DES
Triple Data Encryption Standard（トリプルデータ暗号化標準）

A

ACC
Astaro Command Center

ACPI
Advanced Configuration and Power Interface（アドバンスドコンフィギュレーションアンドパワーインタフェース）

AD
Active Directory

Address Resolution Protocol（アドレス解決プロトコル）
ホストの IP アドレスしかわからない場合に、そのイーサネット MAC アドレスを確定するために使用される。

ADSL
Asymmetric Digital Subscriber Line（非対称デジタル加入者線）

Advanced Configuration and Power Interface（アドバンスドコンフィグレーションアンドパワーインタフェース）
ACPI とは電力管理標準の 1つであり、コンピュータ内の各デバイスに分散させる電力量をオペレーティングシステムで制御できるようにするものです。

Advanced Programmable Interrupt Controller（アドバンスドプログラマブルインタラプトコントローラ）
マルチプロセッサコンピュータシステムでの割り込みを処理するアーキテクチャ。

AES
Advanced Encryption Standard（高度暗号化標準）

AFC
Astaro Flow Classifier

AH
Authentication Header（認証ヘッダ）

AMG
Astaro Mail Gateway

APIC
Advanced Programmable Interrupt Controller（アドバンスドプログラマブルインタラプトコントローラ）

ARP
Address Resolution Protocol（アドレス解決プロトコル）

AS
Autonomous System（自律システム）

ASCII
American Standard Code for Information Interchange（情報交換用米国標準コード）

ASG
Astaro Security Gateway

Astaro Command Center
複数の Astaro ゲートウェイ装置を 1つのインタフェースで監視管理するためのソフトウェア。バージョン 4 より、Sophos UTM Manager（SUM）に名前が変更されました。

Astaro Security Gateway
メールと Web セキュリティを含む、統合脅威管理のためのソフトウェア。バージョン 9 より、Unified Threat Management（UTM）に名前が変更されました。

Authentication Header（認証ヘッダ）
アンチリプレイを提供し、伝送中にパケットの内容が改ざんされていないことを検

証するIPSecプロトコル。

Autonomous System（自律システム）
1つのエンティティによって管理されるIPネットワークとルータの集合体であり、インターネットに対して共通のルーティングポリシーを持つ。

AWG
Astaro Web Gateway

AWS
Amazon Web Services

B

BATV
Bounce Address Tag Validation（バウンスアドレスタグ検証）

BGP
Border Gateway Protocol

Bounce Address Tag Validation（バウンスアドレスタグ検証）
メールメッセージに指定された返信アドレスが有効であるかどうかを判定するために規定された手法の名前。偽造された返信アドレスへのバウンスメッセージを拒否するように設計されている。

C

CA
認証局（CA）

CBC
Cipher Block Chaining（暗号ブロック連鎖）

CDMA
Code Division Multiple Access（符号分割多重アクセス）

Certificate Authority（認証局）
他のパーティによって使用されるデジタル証明書を発行する団体または組織。

CHAP
Challenge-Handshake Authentication Protocol（チャレンジハンドシェイク認証プロトコル）

Cipher Block Chaining（暗号ブロック連鎖）
暗号処理モードの1つであり、平文（プレーンテキスト）の各ブロックを直前の暗号文ブロックと「排他的論理和（XOR）」してから暗号化する。これにより、暗号文の各ブロックはその時点までのすべての平文ブロックに依存するようになる。

CMS
Content Management System（コンテンツ管理システム）

CPU
Central Processing Unit（中央処理装置）

CRL
Certificate Revocation List（証明書失効リスト）

CSS
Cascading Style Sheets（カスケーディングスタイルシート）

D

DC
Domain Controller（ドメインコントローラ）

DCC用
Direct Client Connection（直接クライアント接続）

DDoS
Distributed Denial of Service（分散型サービス拒否）

DER
Distinguished Encoding Rules（識別符号化規則）

Destination Network Address Translation（宛先ネットワークアドレス変換）
データパケットの宛先アドレスを書き換える特殊な NAT。

DHCP
Dynamic Host Configuration Protocol（ダイナミックホスト設定プロトコル）

Digital Signature Algorithm（デジタル署名アルゴリズム）
米国連邦政府が推奨しているデジタル署名についての標準（FIPS）。

Digital Subscriber Line（デジタル加入者線）
地域電話網のケーブル上でのデジタルデータ伝送を提供する技術群。

Distinguished Encoding Rules（識別符号化規則）
X.509 証明書などデジタル署名または署名が検証されるデータオブジェクトを符号化するための方式。

DKIM
Domain Keys Identified Mail（ドメインキー識別メール）

DMZ
Demilitarized Zone（非武装地帯）

DN
Distinguished Name（識別名）

DNAT
Destination Network Address Translation（宛先ネットワークアドレス変換）

DNS
Domain Name Service（ドメインネームサービス）

DOI
Domain of Interpretation（解釈ドメイン）

Domain Name Service（ドメインネームサービス）
インターネットを介して接続されたコンピュータの基底の IP アドレスを、人にとってわかりやすい名前やエイリアスに変換する。

DoS
Denial of Service（サービス拒否）

DSA
Digital Signature Algorithm（デジタル署名アルゴリズム）

DSCP
Differentiated Services Code Point（差別化サービスコードポイント）

DSL
Digital Subscriber Line（デジタル加入者線）

DUID
DHCP Unique Identifier（DHCP 固有識別子）

Dynamic Host Configuration Protocol（ダイナミックホスト設定プロトコル）
ネットワーク上のデバイスがIPアドレスを取得するために使用するプロトコル。

E

ECN
Explicit Congestion Notification（明示的な輻輳通知）

Encapsulating Security Payload（カプセル化セキュリティペイロード）
データの機密性（暗号）、アンチリプレイ、認証を提供する IPSec プロトコル。

ESP
Encapsulating Security Payload（カプセル化セキュリティペイロード）

Explicit Congestion Notification（明示的な輻輳通知）
明示的な輻輳通知（ECN）とはインターネットプロトコルの拡張であり、ネットワーク輻輳のエンドツーエンドな通知をパケットのドロップなしで許可します。ECNは、接続の両エンドポイントの間で使用のネゴシエートが成功している場合にのみ機能します。

F

FAT
File Allocation Table（ファイルアロケーションテーブル）

File Transfer Protocol（ファイル転送プロトコル）
パケット交換網上でのファイル交換用プロトコル。

FQHN
Fully Qualified HostName（完全修飾ホスト名）

FTP
File Transfer Protocol（ファイル転送プロトコル）

G

Generic Routing Encapsulation（ジェネリックルーティングカプセル化）
任意のネットワーク層パケット内で任意のネットワーク層パケットをカプセル化するために規定されたトンネリングプロトコル。

GeoIP
衛星画像を使用して世界中のデバイスの位置を特定する技術。

GRE
Generic Routing Encapsulation（ジェネリックルーティングカプセル化）

GSM
Global System for Mobile Communications（汎欧州デジタル移動電話方式）

H

H.323
パケット交換網上での音声・映像通信セッションを提供するプロトコル。

HA
冗長化（HA）

HCL
Hardware Compatibility List（ハードウェア互換性リスト）

HELO
SMTP（Simple Mail Transfer Protocol: 簡易メール転送プロトコル）のコマンドであり、クライアントはこれを使用してサーバからの初期グリーティングに応答します。

HIPS
Host-based Intrusion Prevention System（ホストベースの侵入防止システム）

HMAC
Hash-based Message Authentication Code（ハッシュベースのメッセージ認証コード）

HTML
Hypertext Transfer Markup Language（ハイパーテキスト転送マークアップ言語）

HTTP
Hypertext Transfer Protocol（ハイパーテキスト転送プロトコル）

HTTP over SSL
よりセキュアな HTTP 通信を実現するプロトコル。

HTTP/S
Hypertext Transfer Protocol Secure（ハイパーテキスト転送プロトコルセキュア）

HTTPS
Hypertext Transfer Protocol Secure（ハイパーテキスト転送プロトコルセキュア）

Hypertext Transfer Protocol（ハイパーテキスト転送プロトコル）
インターネット上で情報を転送するためのプロトコル。

I

IANA
Internet Assigned Numbers Authority（インターネット番号割当当局）

ICMP
Internet Control Message Protocol（インターネット制御メッセージプロトコル）

ID
Identity（アイデンティティ）

IDE
Intelligent Drive Electronics（インテリジェントドライブエレクトロニクス）

IDENT
特定の TCP 接続のユーザを特定するための標準プロトコル。

IDN
International Domain Name（国際ドメイン名）

IE
Internet Explorer

IKE
Internet Key Exchange（インターネット鍵交換）

IM
Instant Messaging（インスタントメッセージング）

Internet Control Message Protocol（インターネット制御メッセージプロトコル）
ネットワークのステータスやその他のコントロール情報についての情報を送受信するために使用される特別な IP プロトコル。

Internet Protocol（インターネットプロトコル）
パケット交換網上でのデータ通信に使用されるデータ指向プロトコル。

Internet Relay Chat（インターネットリレーチャット）
インターネット上でのインスタント通信を可能にするオープンプロトコル。

IP
Internet Protocol（インターネットプロトコル）

IP アドレス
インターネットプロトコル標準を使用するコンピュータネットワーク上の各デバイスが互いを特定し、通信するために使用する一意の番号。

IPS
IPS（侵入防御システム）

IPsec
Internet Protocol Security（インターネットプロトコルセキュリティ）

IRC
Internet Relay Chat（インターネットリレーチャット）

ISP
Internet Service Provider（インターネットサービスプロバイダ）

L

L2TP
Layer Two (2) Tunneling Protocol（レイヤ 2 トンネリングプロトコル）

LAG
Link Aggregation Group（リンクアグリゲーショングループ）

LAN
Local Area Network（ローカルエリアネットワーク）

LDAP
Lightweight Directory Access Protocol（ライトウェイトディレクトリアクセスプロトコル）

Link-state advertisement（リンクステートアドバタイズメント）
IP 用の OSPF ルーティングプロトコルの基本的な通信手段。

LSA
Link-state advertisement（リンクステートアドバタイズメント）

LTE
3GPP Long Term Evolution（3GPP ロングタームエボリューション）

M

MAC
Media Access Control（メディアアクセスコントロール）

MAC アドレス
ほとんどの形態のネットワークハードウェアに割り当てられる一意のコード。

Management Information Base（管理情報ベース）
通信ネットワーク内のデバイスを管理するために使用されるデータベースの種類。ネットワーク内のエンティティ（ルータやスイッチなど）を管理するために使用される（仮想）データベース内のオブジェクトの集合から構成される。

MD5
Message-Digest algorithm 5（メッセージダイジェストアルゴリズム 5）

Message-Digest algorithm 5（メッセージダイジェストアルゴリズム 5）
128ビットのハッシュ値による暗号ハッシュ関数。

MIB
Management Information Base（管理情報ベース）

MIME タイプ
Multipurpose Internet Mail Extensions（多目的インターネットメール拡張）

MPLS
Multiprotocol Label Switching（マルチプロトコルラベルスイッチング）

MPPE
Microsoft Point-to-Point Encryption（マイクロソフトポイントツーポイント暗号化）

MSCHAP
Microsoft Challenge Handshake Authentication Protocol（マイクロソフトチャレンジハンドシェイク認証プロトコル）

MSCHAPv2
Microsoft Challenge Handshake Authentication Protocol Version 2（マイクロソフトチャレンジハンドシェイク認証プロトコルバージョン2）

MSP
マネージド サービス プロバイダ

MSSP
マネージドセキュリティサービスプロバイダ

MTU
Maximum Tansmission Unit（最大伝送単位）

Multipurpose Internet Mail Extensions（多目的インターネットメール拡張）
メールのフォーマットを拡張し、US-ASCII 以外の文字セットのテキスト、テキスト以外の添付物、マルチパートメッセージ本

体、ASCII 以外の文字セットでのヘッダ情報をサポートするためのインターネット標準。

MX レコード
インターネットでメールをどのようにルーティングするのかを指定する、ドメインネームシステム (DNS) 内のリソースレコードの種類。

N

NAS
Network Access Server (ネットワークアクセスサーバ)

NAT
Network Address Translation (ネットワークアドレス変換)

NAT-T
NAT Traversal (NAT トラバーサル)

Network Address Translation (ネットワークアドレス変換)
IP アドレスを再利用するためのシステム。

Network Time Protocol (ネットワークタイムプロトコル)
パケット交換網上でコンピュータシステムのクロックを同期するためのプロトコル。

NIC
Network Interface Card (ネットワークインタフェースカード)

Not-so-stubby area (Not-so-stubby エリア)
OSPF プロトコルの中で、自律システム (AS) 外部ルートをインポートし、それらをバックボーンに送信することはできるが、バックボーンやその他のエリアから AS 外部ルートを受信することはできないタイプのスタブエリア。

NSSA
Not-so-stubby area (Not-so-stubby エリア)

NTLM
NT LAN Manager (Microsoft Windows)

NTP
Network Time Protocol (ネットワークタイムプロトコル)

O

Open Shortest Path First (オープンショーテストパスファースト)
ネットワークルーティングのための、リンクステート型の階層的な IGP (interior gateway protocol)。

OpenPGP
強力な公開鍵と対称暗号を組み合わせて、電子通信とデータストレージのためのセキュリティサービスを提供するプロトコル。

OSI
Open Source Initiative (オープンソースイニシアチブ)

OSPF
Open Shortest Path First (オープンショーテストパスファースト)

OU
Organisational Unit (組織単位)

P

PAC
Proxy Auto Configuration (プロキシの自動設定)

PAP
Password Authentication Protocol (パスワード認証プロトコル)

PCI
Peripheral Component Interconnect (ペリフェラルコンポーネントインターコネクト)

PEM
Privacy Enhanced Mail (プライバシー拡張メール)

PGP
Pretty Good Privacy (プリティグッドプライバシー)

PKCS
Public Key Cryptography Standards (公開鍵暗号標準)

PKI
Public Key Infrastructure (公開鍵暗号基盤)

PMTU
Path Maximum Transmission Unit (パス最大伝送単位)

POP3
Post Office Protocol version 3 (ポストオフィスプロトコルバージョン3)

Post Office Protocol version 3 (ポストオフィスプロトコルバージョン3)
パケット交換網上でメールを配信するためのプロトコル。

PPP
Point-to-Point Protocol (ポイントツーポイントプロトコル)

PPPoA
PPP over ATM Protocol (PPP オーバー ATMP プロトコル)

PPTP
Point to Point Tunneling Protocol (ポイントツーポイントトンネリングプロトコル)

Privacy Enhanced Mail (プライバシー拡張メール)
公開鍵暗号を使用してメールのセキュリティを保護するための、初期の IETF 提案。

PSK は除きます。
事前共有鍵 (Preshared Key)

Q

QoS
Quality of Service (サービス品質)

R

RADIUS
Remote Authentication Dial In User Service (リモート認証ダイヤルインユーザサービス)

RAID
Redundant Array of Independent Disks (独立ディスク冗長アレイ)

RAM
Random Access Memory (ランダムアクセスメモリ)

RAS
Remote Access Server (リモートアクセスサーバ)

RBL
Realtime Blackhole List (リアルタイムブラックホールリスト)

RDN
Relative Distinguished Name (相対識別名)

RDNS
Reverse Domain Name Service (リバースドメインネームサービス)

RDP
Remote Desktop Protocol (リモートデスクトッププロトコル)

RED
Random Early Detection (ランダム初期検知)

Redundant Array of Independent Disks（独立ディスク冗長アレイ）
複数のハードドライブを使用してドライバ間でデータを共有または複製するデータ保管スキーム。

Remote Authentication Dial In User Service（リモート認証ダイヤルインユーザサービス）
ルータなどのネットワークデバイスが中央データベースに対してユーザを認証できるように設計されたプロトコル。

RFC
Request for Comment（リクエストフォーコメント）

RPS
RED プロビジョニングサービス

RSA
Rivest, Shamir, & Adleman（リベスト、シャミア、エーデルマン: 公開鍵暗号化技術）

S

S/MIME
Secure/Multipurpose Internet Mail Extensions（セキュア多目的インターネットメール拡張）

SA
Security Associations（セキュリティアソシエーション）

SAA
Sophos Authentication Agent（ソフォス認証エージェント）

SCP
Secure Copy（セキュアコピー: セキュア通信用の SSH コンピュータアプリケーションスイートからの）

SCSI
Small Computer System Interface（スモールコンピュータシステムインタフェース）

Secure Shell（セキュアシェル）
異なるパケット交換網にまたがるローカルコンピュータとリモートコンピュータの間でセキュアなチャネルを確立するためのプロトコル。

Secure Sockets Layer（セキュアソケットレイヤ）
インターネット上でセキュアな通信を提供する暗号プロトコル。TLS（トランスポートレイヤセキュリティ）の前身である。

Secure/Multipurpose Internet Mail Extensions（セキュア多目的インターネットメール拡張）
MIME にカプセル化されたメールに対する公開鍵暗号化や署名のための標準。

Security Parameter Index（セキュリティパラメータインデックス）
IP トラフィックのトンネリングに IPSec を使用するときにヘッダに追加される識別タグ。

Sender Policy Framework（送信者ポリシーフレームワーク）
SMTP（Simple Mail Transfer Protocol: 簡易メール転送プロトコル）の拡張。SPF を使用すると、スパムによく見られる SMTP MAIL FROM（リターンパス）の偽造アドレスをソフトウェアで特定し、拒否することができる。

Session Initiation Protocol（セッション開始プロトコル）
2つ以上の通信パートナー間でセッションを確立、変更、終了するためのシグナリングプロトコル。このテキスト指向のプロトコルは HTTP をベースとしており、IP ネットワーク経由でTCPまたは UDP を通して信号データを送信できる。そのため、VoIP（Voice-over-IP）ビデオ電話やリアルタイムなマスチメディアサービスなどの基盤となる。

SFQ
Stochastic Fairness Queuing（確率的不偏キューイング）

SIM
Subscriber Identification Module

Simple Mail Transfer Protocol (簡易メール転送プロトコル)
パケット交換網上でメールを送受信するために使用されるプロトコル。

Single sign-on (シングルサインオン)
ユーザが一度だけ認証を行い、1つのパスワードを使用して複数のアプリケーションやシステムにアクセスできるようにする認証方式。

SIP
Session Initiation Protocol (セッション開始プロトコル)

SLAAC
Stateless Address Autoconfiguration (ステートレスアドレス自動設定)

SMB
Server Message Block (サーバメッセージブロック)

SMP
Symmetric Multiprocessing (対称型マルチプロセッシング)

SMTP
Simple Mail Transfer Protocol (簡易メール転送プロトコル)

SNAT
Source Network Address Translation (送信元ネットワークアドレス変換)

SNMP
Simple Network Message Protocol (シンプルネットワークメッセージプロトコル)

SOCKetS
クライアントサーバアプリケーションがネットワークファイアウォールのサービスを透過的に使用できるようにするインターネットプロトコル。現在、SOCKS (別名: ファイアウォールトラバースプロトコル) はバージョン 5 であり、正しく機能するためにはクライアント側のプログラムに導入する必要がある。

SOCKS
SOCKetS

Sophos UTM Manager
複数の UTM 装置を 1つのインタフェースで監視管理するためのソフトウェア。(旧製品: Astaro Command Center)。

Source Network Address Translation (送信元ネットワークアドレス変換)
特殊な NAT。SNAT では、接続を開始したコンピュータの IP アドレスが書き換えられる。

Spanning Tree Protocol (スパニングツリープロトコル)
ブリッジのループを検出して回避するネットワークプロトコル

SPF
Sender Policy Framework (送信者ポリシーフレームワーク)

SPI
Security Parameter Index (セキュリティパラメータインデックス)

SSH
Secure Shell (セキュアシェル)

SSID
Service Set Identifier (サービスセット識別子)

SSL
Secure Sockets Layer (セキュアソケットレイヤ)

SSO
Single sign-on (シングルサインオン)

STP
Spanning Tree Protocol（スパニングツリープロトコル）

SUA
Sophos User Authentication（ソフォスユーザ認証）

SUM
Sophos UTM Manager

Symmetric Multiprocessing（対称型マルチプロセッシング）
複数 CPU を使用すること。

SYN
Synchronous（同期）

T

TACACS
Terminal Access Controller Access Control System（ターミナルアクセスコントローラアクセスコントロールシステム）

TCP
Transmission Control Protocol（伝送制御プロトコル）

TFTP
Trivial File Transfer Protocol（簡易ファイル転送プロトコル）

Time-to-live（生存時間）
IP（インターネットプロトコル）ヘッダ内の 8 ビットのフィールドであり、パケットをネットワーク経由で伝送できる制限時間を指定する。この時間が経過すると、そのパケットは廃棄される。

TKIP
Temporal Key Integrity Protocol（一時鍵完全性プロトコル）

TLS
Transport Layer Security（トランスポートレイヤセキュリティ）

TOS
Type of Service（サービスタイプ）

Transmission Control Protocol（伝送制御プロトコル）
インターネットプロトコルスイートのプロトコル。これにより、ネットワーク内のコンピュータ上のアプリケーションが相互接続できる。このプロトコルによって、データが送信者から受信者へ確実かつ順序通りに送信される。

Transport Layer Security（トランスポートレイヤセキュリティ）
インターネット上でセキュアな通信を提供する暗号プロトコル。SSL（セキュアソケットレイヤ）の後継プロトコルである。

TTL
Time-to-live（生存時間）

U

UDP
User Datagram Protocol（ユーザデータグラムプロトコル）

UMTS
Universal Mobile Telecommunications System（ユニバーサル移動体通信システム）

Unified Threat Management
メールと Web セキュリティを含む、統合脅威管理のためのソフトウェア。（旧製品: Astaro Security Gateway）。

Uniform Resource Locator（ユニフォームリソースロケータ）
インターネット上のリソースの位置を指定する文字列。

Up2Date
Sophos サーバから関連する更新パッケージをダウンロードするためのサービス。

UPS
Uninterruptible Power Supply（無停電電源装置）

URL
Uniform Resource Locator（ユニフォームリソースロケータ）

USB
Universal Serial Bus（ユニバーサルシリアルバス）

User Datagram Protocol（ユーザデータグラムプロトコル）
ネットワーク上のコンピュータのアプリケーションで短いメッセージ（別名：データグラム）をやりとりするためのプロトコル。

UTC
Coordinated Universal Time（協定世界時）

UTM
Unified Threat Management

V

VDSL
Very High Speed Digital Subscriber Line（超高速デジタル加入者線）

Virtual Private Network（バーチャルプライベートネットワーク）
公衆通信インフラを利用するプライベートデータネットワーク。PPTP や IPSec などのトンネリングプロトコルを使用してプライバシーを維持する。

VLAN
Virtual LAN（バーチャル LAN）

VNC
Virtual Network Computing（仮想ネットワークコンピューティング）

Voice over IP（ボイスオーバー IP）
インターネット上またはその他の IP ベースのネットワーク上での音声会話ルーティング。

VoIP
Voice over IP（ボイスオーバー IP）

VPC
Virtual Private Cloud（バーチャルプライベートクラウド）

VPN
Virtual Private Network（バーチャルプライベートネットワーク）

W

WAF
Web アプリケーション ファイアウォール

WAN
Wide Area Network（ワイドエリアネットワーク）

W-CDMA
Wideband Code Division Multiple Access（広帯域符号分割多重アクセス）

WebAdmin
UTM、SUM、ACC、ASG、AWG、および AMG などの Sophos/Astaro 製品用の Web ベース GUI。

WEP
Wired Equivalent Privacy（有線同等機密）

Windows Internet Naming Service（Windows インターネットネーミングサービス）
マイクロソフトが Windows に実装した NBNS（NetBIOS Name Server: NetBIOS ネームサーバ）。NetBIOS コンピュータ名のためのネームサーバおよびサービスである。

WINS
Windows Internet Naming Service（Windows インターネットネーミングサービス）

WLAN
Wireless Local Area Network（無線 LAN）

WPA
Wi-Fi Protected Access (Wi-Fi 保護アクセス)

X

X.509
ITU-T (国際電気通信連合、電気通信標準化部門) が公開したデジタル証明書の仕様。個人またはコンピュータシステムの識別に必要な情報や属性を規定する。

XSS
Cross-site scripting (クロスサイトスクリプティング)

イ

インターネットサービスプロバイダ
インターネットや関連サービスへのアクセスを利用者に販売する企業または組織。

ク

クラスタ
リンクされたコンピュータのグループ。緊密に連携して多くの局面で 1台のコンピュータとして機能する。

サ

サブネットマスク
ネットワークのサブネットマスク (別名: ネットマスク) とネットワークアドレスによって、ローカルネットワークの一部となるアドレスとならないアドレスが定義される。個々のコンピュータは、この定義に基づいてネットワークに割り当てられる。

デ

デバイスツリー
メインメニューの下にあり、SUM に登録されたすべてのゲートウェイ装置にアクセス権を付与する。

ブ

ブロードキャスト
ネットワーク内の他のすべてのコンピュータに向けてメッセージを一括送信するためにコンピュータで使用されるアドレス。たとえば、IP アドレスが 192.168.2.0 でネットワークマスクが 255.255.255.0 のネットワークは、ブロードキャストアドレスが 192.168.2.255 となる。

プ

プロキシ
クライアントが他のネットワークサービスに対して間接的にネットワーク接続できるようにするコンピュータネットワークサービスを提供するコンピュータ。

プロトコル
2つのコンピュータエンドポイント間での接続、通信、データ転送を制御または実現するための、明確で標準化されたルールセット。

ポ

ポート
データを直接交換するためにプログラムで使用できる仮想データ接続。具体的には、ポートとは追加の識別子である (TCP と UDP の場合、0～65535 の番号)。これにより、コンピュータはある 2台のコンピュータ間に存在する複数の同時接続を見分けることができる。

ポートスキャン
ネットワークホストの空きポートを探す行為。

マ

マスカレード
LAN 全体で 1つのパブリック IP アドレスを使用してインターネットの他の部分と通信できるようにする NAT ベースの技術。

マネージドセキュリティサービスプロバイダ
企業に対してセキュリティサービスを提供する。

リ

リアルタイムブラックホールリスト
スパム行為に関与しているIP アドレスのリストをインターネットサイトが公開できる手段。ほとんどのメール転送エージェント（メールサーバ）ソフトウェアは、1つ以上のブラックホールリストに記載されたサイトから送信されたメッセージを拒否したりフラグを付加したりするように設定できる。Web サーバも、RBL に掲載されているクライアントを拒否することができます。

ル

ルータ
最も効率の良いパスで宛先までパケットを転送するために指定されるネットワークデバイス。

共

共有シークレット
セキュア通信の 2つのエンティティ間で共有されているパスワードまたはパスフレーズ。

冗

冗長化（HA）
信頼できるレベルの運用継続性を確実に保証するためのシステム設計プロトコル。

無

無停電電源装置
接続された機器に対する継続的な配電を維持するためのデバイス。通常電源を使用できないときには別の電源から電力を供給する。

図の一覧

Figure 1 WebAdmin:初期ログインページ 23
Figure 2 WebAdmin:通常のログインページ 24
Figure 3 WebAdmin:ダッシュボード 26
Figure 4 WebAdmin:概要 29
Figure 5 WebAdmin:リストの例 32
Figure 6 WebAdmin:ダイアログボックスの例 34
Figure 7 WebAdmin:オブジェクトリスト ネットワークからオブジェクトをドラッグする 37
Figure 8 MyAstaroポータル 60
Figure 9 ライセンス:サブスクリプション警告メッセージ 64
Figure 10 Up2Date:進捗ウィンドウ 67
Figure 11 ユーザポータル:Welcomeページ 75
Figure 12 カスタマイズ:ブロックされるページの例とカスタマイズ可能な部分 81
Figure 13 カスタマイズ:HTTP ダウンロードページ、ステップ1/3ファイルダウンロード中 84
Figure 14 カスタマイズ:HTTP ダウンロードページ、ステップ2/3ウイルススキャン中 85
Figure 15 カスタマイズ:HTTP ダウンロードページ、ステップ3/3ファイルのダウンロード完了 85
Figure 16 カスタマイズ:POP3プロキシのブロックメッセージ 87
Figure 17 グループ: Sophos UTM 115
Figure 18 認証:Microsoft Management Console 122
Figure 19 メール暗号化:2つのSophos UTMユニットの使用 327
Figure 20 メールマネージャ – Sophos UTM 339
Figure 21 エンドポイントプロテクション:概要 348
Figure 22 メッシュネットワークの使用例 – ワイヤレスブリッジ 378
Figure 23 メッシュネットワークの使用例 – ワイヤレスリピーター 379
Figure 24 RED:セットアップの略図 401
Figure 25 RED 50:ホスト名とアップリンクとも分散(青緑)およびホスト名とアップリンクともフェイルオーバー(赤) 410
Figure 26 RED 50:ホスト名の分散とアップリンクのフェイルオーバー(緑)およびホスト名のフェイルオーバーとアップリンクの分散(青) 410
Figure 27 レポーティング:折れ線グラフの例 476
Figure 28 レポーティング:円グラフの例 476